Key Bridge Global LLC
1600 Tysons Blvd., Suite 450
McLean, VA 22102
Tel: 703 414 3500
Fax: 703 414 3501

Proposal to Administer a TV Bands Database

Revised

Response to DA 09-2479
ET Docket No. 04-185

Document Information

Document Status	Public. Updated to comply with final Rules, Errata and Designation conditions as specified in the following documents: DA 09-2479 Invitation for Proposal, rel. 11/25/2009 FCC 10-174 Second Memorandum Opinion & Order, rel. 09/23/2010 DA 11-131 Conditionally Designating Order, rel. 01/26/2011
Date Printed:	February 25, 2011
Copyright	

1 Table of Contents

2 Overview and Opening Statement

The Key Bridge Team is pleased to submit this revised proposal to administer a database of the unlicensed Television broadcast bands which has been updated to comply with the final Rules. The companies and technologies brought together in our solution are proven and known to work together. In fact, the architecture, components and services in the Key Bridge Team's white space administration solution currently support millions of network users and billions of dollars in online commerce safely, securely and reliably.

Key Bridge is also pleased to welcome Symantec to our solution team. Symantec, a leading provider of computer security software, is also a leading provider of embedded digital certificate technology and leading operator of global public key infrastructure. Symantec's vast experience with embedded digital certificates, identity management and global security services will provide great value to the White Space ecosystem and serve to further accelerate its time to market.

The Key Bridge Team's solution meets or exceeds all of the Commission's present requirements and is flexible enough to accommodate whatever future changes or modifications to those requirements the Commission may require. We are happy to provide any additional information the Commission may require.

Jesse Caulfield

President & CEO, Key Bridge Global LLC

Key Bridge Team Leader

Amazon Web Services	*Key Bridge Global LLC*	*Symantec Inc.*
Equinix Inc.	*Level (3) Communications*	
Fortinet Inc.	*Oracle Inc.*	

2.1 Statement of Acceptance of Designating Conditions

In its January 26 Order designating all 9 applicants as TV bands database administrators the Commission enumerated certain conditions. These are:

1. Administrators must supplement their previous filings with sufficient detailed information to indicate how it will comply with the rule changes adopted in the *Second MO&O* (FCC 10-174).
2. Administrators must attend [one or more] workshops to be conducted by OET to address database operations; to ensure consistency; and to ensure compliance with the Rules. Each administrator must also designate a Responsible Party who will represent the organization.
3. Administrators must cooperation with any steps OET may deem necessary to ensure Rules compliance.
4. Each administrator must agree that they will not engage in any discriminatory or anti-competitive practices or any practices that may compromise the privacy of users.

2.1.1 Condition 1: Supplement Previous Filings to Indicate Compliance

This document, *Proposal to Administer Unlicensed TV Bands (Revised)*, shall serve as the Key Bridge Team's supplement to our previous filing. Throughout this document various sections have been updated and certain approaches have been modified to bring them into compliance with the final Rules.

Certain products identified in our original proposal have become outdated, and these sections have been updated to a more general, and less product-centric, discussion.

Our original proposal did provide a robust security framework and options for strong authentication, data encryption and identity management. However, these aspects of our proposal were considered optional as the Rules did not specifically address or require the security technologies we promoted. In this revised document we have taken a fresh look at information assurance and end-to-end system security given the Rules' specific requirements for identify management and end-to-end data integrity. We now identify and specify the use of certain technologies that were previously optional, for example digital certificated and public key infrastructure, which honors the Rules' intent, may be readily implemented and impose minimal cost or burden on unlicensed devices, operators and consumers.

We have also revised sections that describe selection of CDBS and ULS database records for protection, protected entity registration, LPAUX protections, database synchronization, treatment of US-Mexico and Canada border protection.

We also include revised thinking about the encoding and framing of channel list transactions.

2.1.2 Condition 2: Designation of Responsible Party

We are very grateful to have received a vote of confidence by the Commission's Office of Engineering and Technology to have been conditionally designated a TV bands database administrator.

At the scheduled workshops and throughout the process of testing, evaluation and trial our designated responsible party and interlocutor with the FCC is:

Mr. Jesse Caulfield, President

Key Bridge Global LLC

1600 Tysons Blvd., Suite 450

McLean, VA 22102

Tel: (703) 414-3500

Fax: (703) 414-3501

Email: jesse.caulfield@keybridgeglobal.com

Key Bridge and the solution team we represent look forward to working with the FCC and the other conditionally designated administrators in the coming weeks and months to make this important undertaking a runaway success.

2.1.3 Condition 3: Cooperation to Ensure Rules Compliance

Key Bridge is committed to cooperate with the FCC and stands ready to incorporate whatever modifications the Commission may deem necessary to ensure our systems and services are in compliance with the rules. We are also prepared to accommodate whatever reasonable and objective testing methods and procedures the Commission may deem necessary to ensure the safety, security and reliability of our systems and services.

2.1.4 Condition 4: Declaration of Commitment to Non-Discrimination

Key Bridge hereby restates our strong commitment to neutral spectrum administration. Key Bridge understands the purpose and requirements for administering unlicensed operation in the television broadcast bands are as follows:

- Protect licensed services from interference through accurate and timely implementation of geographic spectrum sharing strategies
- Publish unlicensed spectrum available for unlicensed access on a non-discriminatory basis regardless of type of service, device, user, location, or any other use characteristic
- Provide convenient, accurate and timely information services to all administrator users

- Encourage white space adoption by maximizing consumer convenience and spectrum transparency

Accordingly, Key Bridge confirms that we, our contractors, associates, successors and assigns, will not use our capacity as a database manager to engage in any discriminatory or anti-competitive practices or any practices that my compromise the privacy of Database users.

Sincerely

/s/

Jesse Caulfield

President & CEO, Key Bridge Global LLC

Key Bridge Team Leader

2.2 Enumerated FCC Database Requirements (from FCC 10-174: Code of Federal Regulations)

Title 47: Telecommunication

PART 15—RADIO FREQUENCY DEVICES

Subpart H—Television Band Devices

§ 15.713 TV bands database.

(a) Purpose. The TV bands database serves the following functions:

(1) To determine and provide to a TVBD, upon request, the available TV channels at the TVBD's location. Available channels are determined based on the interference protection requirements in §15.712.

...[To provide] TVBDs with channel availability information that includes scheduled changes in channel availability over the course of the 48 hour period beginning at the time the TVBDs make a re-check contact.

...[To] ensure that all communications and interactions between the TV bands database and the TVBD include adequate security measures such that unauthorized parties cannot access or alter the TV bands database or the list of available channels sent to TVBDs or otherwise affect the database system or TVBDs in performing their intended functions or in providing adequate interference protections to authorized services operating in the TV bands.

...[To] verify that the FCC identifier (FCC ID) of a device seeking access to its services is valid; under this requirement the TV bands database must also verify that the FCC ID of a Mode I device provided by a fixed or Mode II device is valid.

(2) To register the identification information and location of fixed TVBDs.

(3) To register protected locations and channels as specified in paragraph (b)(2) of this section, that are not otherwise recorded in Commission licensing databases.

(i) Commission requests for data.

1) A TV bands database administrator must supply upon request by the Commission, any information contained in the database.

2) A TV bands database administrator must remove information from the database, upon direction, in writing, by the Commission.

(j) Security. The TV bands database shall employ protocols and procedures to ensure that all communications and interactions between the TV band database and TVBDs are accurate and secure and that unauthorized parties cannot access or alter the database or the list of available channels sent to a TVBD.

(i) Communications between TV band devices and TV bands databases, and between different TV bands databases, shall be secure to prevent corruption or unauthorized interception of data. A TV bands database shall be protected from unauthorized data input or alteration of stored data.

(ii) A TV bands database shall verify that the FCC identification number supplied by a fixed or personal/portable TV band device is for a certified device and may not provide service to an uncertified device.

(iii)A TV bands database must not provide lists of available channels to uncertified TV bands devices for purposes of operation (it is acceptable for a TV bands database to distribute lists of available channels by means other than contact with TVBDs to provide list of channels for operation). To implement this provision, a TV bands database

administrator shall obtain a list of certified TVBDs from the FCC Equipment Authorization System.

§ 15.715 TV bands database administrator.

The Commission will designate one or more entities to administer a TV bands database. Each database administrator shall:

a) *Maintain a database that contains the information described in Section 15.713 of this part.*

b) *Establish a process for downloading and storing in the database necessary and appropriate information from the Commission's databases and synchronizing the TV bands database with the current Commission databases at least once a week to include newly licensed facilities or any changes to licensed facilities.*

c) *Establish a process for registering fixed TVBDs and registering and including in the database facilities entitled to protection but not contained in a Commission database, including MVPD and TV translator receive sites.*

d) *Establish a process for registering facilities where Part 74 low power auxiliary stations are used on a regular basis.*

e) *Provide accurate lists of available channels to fixed and personal/portable TVBDs that submit to it the information required under §§ 15.713(e), (f), and (g) based on their geographic location and provide accurate lists of available channels to fixed and Mode II devices requesting lists of available channels for Mode I devices. Database administrators may allow prospective operators of TV bands devices to query the database and determine whether there are vacant channels at a particular location.*

f) Establish protocols and procedures to ensure that all communications and interactions between the TV band database and TVBDs are accurate and secure and that unauthorized parties cannot access or alter the database or the list of available channels sent to a TVBD consistent with the provisions of Section 15.713(i).

g) Make its services available to all unlicensed TV band device users on a non-discriminatory basis.

h) Provide service for a five-year term. This term can be renewed at the Commission's discretion.

i) Respond in a timely manner to verify, correct and/or remove, as appropriate, data in the event that the Commission or a party brings claim of inaccuracies in the database to its attention. This requirement applies only to information that the Commission requires to be stored in the database.

j) Transfer its database along with the IP addresses and URLs used to access the database and list of registered Fixed TVBDs, to another designated entity in the event it does not continue as the database administrator at the end of its term. It may charge a reasonable price for such conveyance.

k) The database must have functionality such that upon request from the Commission it can indicate that no channels are available when queried by a specific TVBD or model of TVBDs.

l) If more than one database is developed, the database administrators shall cooperate to develop a standardized process for providing on a daily basis or more often, as appropriate, the data collected for the facilities listed in § 15.713(b)(2) to all other TV bands databases to ensure consistency in the records of protected facilities.

2.3 Enumerated FCC Proposal Requirements (from DA 09-2479: Request for Proposal)

Proposals must:

- Address how the basic components of a TV band database(s) will be satisfied
    - i.e., A data repository
    - A data registration process
    - A query process—and
- Address whether the proponent seeks to provide all or only some of these functions
- Affirm that the database service will comply with all of the applicable rules

Proposals must include the following information:

- Demonstrate sufficient technical expertise to administer a TV band database
- Demonstrate a viable business plan to operate for five-year term
- Describe the fee collection process from registrations or queries
- Describe the scope of the database functions that it intends to perform, such as:
    - Managing a data repository
    - Performing calculations to determine available channels
    - Registering fixed unlicensed devices
    - Registering licensed services not listed in the Commission's databases
    - *How functions are performed by another entity*
- Describe data synchronization between multiple databases
- Describe how quickly this synchronization of data will be accomplished
- Provide diagrams showing the architecture of the database system

- Describe how each function operates and interacts with the other functions
- *If the entity will not perform all database functions:*
    - *Provide information on the entities operating other functions*
    - *Describe the business relationship between itself and these other entities*
    - *Address how administrator requirements are satisfied when functions are divided among multiple entities*
    - *Describe how data is transferred among entities*
    - *Describe how data is transferred among databases*
    - *Describe the schedule of such data transfers (i.e., real-time, once an hour, etc.).*
- Describe the methods (e.g., interfaces, protocols) used by TV band devices to communicate with the database
- Describe procedures to verify that a device can properly communicate with the database
- Describe the security methods to ensure that unauthorized parties
    - Cannot access the database
    - Cannot alter the database
    - Cannot otherwise corrupt the operation of the database system
    - Cannot interrupt the database system from performing its functions
- Describe whether and how verify FCC certification of Mode I personal/portable devices

2.4 Interpretation of FCC Database Requirements

Title 47, Part 15, Subpart H – *Television Band Devices* of the Code of Federal Regulations describes in general the minimum set of functions a TV bands database administrator must

provide and describes several data transactions it must support between the TV bands database ("Database") and various external systems. These services include channel lists for unlicensed TV band devices ("TVBD"), registration of protected entities and the verification their services records plus the support of FCC auditing and enforcement activities.

Appendix C of the Rules published in ET Docket 04-186 explains that the purpose of a TV bands database is to allow "low power unlicensed transmitters to operate in the TV broadcast bands at locations where spectrum is not … used by authorized services."

47 CFR §15.713 further explains that the essential commercial function of a TV bands database is to provide, subject to certain restrictions, an accurate list of TV channels available at a requesting TVBD's geographic location.

For purposes of interference avoidance the Database administrator is required to collect from the Commission, and then to maintain, an accurate copy of records describing the location and transmitting parameters of incumbent fixed transmitters. The administrator must calculate geographic protection contours based on these records and employ those contours to determine available channel lists based on location and time of inquiry.[1]

The administrator must enable the Commission to enforce incumbent protection from interference where necessary. Lastly, the administrator must synchronize certain data with other FCC designated database administrators on a daily basis or more often, as appropriate.

In summary, a TV bands database administrator must satisfy all of the following requirements:

1. **Collect** registered incumbent transmitter data from the FCC at least once per week

[1] Protected contours are detailed in §15.712

2. **Validate** and i**dentify** active protected entity records within the FCC-provided transmitter data
    a. **Convert** all FCC locations to the NAD83 geographic datum where necessary
3. Enable the voluntary **registration** of certain protected entities not already in FCC databases
    a. A**ccommodate** MVPDs, BAS fixed links, LP-AUX microphones, etc.
4. Enable the **registration** of Fixed TV band devices
5. Enable the **verification, correction or removal** of information in the database upon request by the Commission or an [authorized] party.
6. **Synchronize** certain data with other authorized administrators at least every 24 hours
7. Implement algorithms to **calculate protected services contours** for each respective protected entity
8. Implement algorithms to **calculate available channels** for any given location within the United States and its territories, also incorporating time of operation and device type
9. Enable the FCC to **enforce** the denial of channel list services to any specific or model of TV band device
10. Positively **authenticate** the certification and enforcement status of TVBDs
11. Implement a **machine-to-machine communications** capability for TVBD channel-queries
    a. **Accept** channel list inquiries via the Internet from any FCC-certified TV band device
    b. Calculate, construct and communicate a **channel list message** according to an established protocol
12. Implement a **security framework** that protects the TV bands administration system, its operational information services and data, plus end-user devices

13. Implement a security framework that ensures **accurate, secure, unalterable communications** between TVBD and database

We are pleased to propose this comprehensive TV bands administration solution that completely fulfils the Commission's published requirements.

We are also pleased to detail the TV band technologies we have developed over the past year in close collaboration with industry partners and other interested parties.

2.5 Statement of Proposal Scope and Compliance

The Key Bridge TV bands administration solution described herein completely fulfils the Commission's requirements and satisfies all of the requirements stated in the TV bands Rules.

Our flexible, modular solution architecture completely satisfies the FCC's current requirements and can easily accommodate future requirements the Commission may deem necessary.

Requirements Response:

Address how the basic components of a TV band database(s) will be satisfied

Section 4 provides a summary of the Key Bridge Team's end-to-end solution architecture. The Key Bridge TV bands database system is comprehensive and includes all of the components required to provide a high-availability, scalable and standards compliant TV band services.

i.e., A data repository

Section 5 describes the modules and components that constitute the data repository

A data registration process

Protected entities are learned directly from the FCC Data and by voluntary registration. These processes are described in sections 5.4.1 and 5.4.2, respectively.

A query process

Channel list services are described in section 5.4.7.

Address whether the proponent seeks to provide all or only some of these functions

The Key Bridge solution is comprehensive and provides end-to-end service

Affirm that the database service will comply with all of the applicable rules

Our flexible, modular solutions architecture completely satisfies the FCC's current requirements.

Demonstrate sufficient technical expertise to administer a TV band database

The Technologies in this document support millions of users and billions of dollars in online services. The proposing Team includes some of the best and most respected providers of technology, services, infrastructure and operations in the industry.

Demonstrate a viable business plan to operate for five-year term

Section 9 describes the Team's commercialization strategy.

Describe the fee collection process from registrations or queries

Section 9.3 described payment options for registration fees, and section 9.4 describes payment options for channel list fees.

Describe the scope of the database functions that it intends to perform, such as:

The Key Bridge solution is comprehensive and provides end-to-end service. Section 4 provides a summary of the Key Bridge Team's solution architecture. The Key Bridge TV bands database system includes is comprehensive and includes all of the components required to provide high-availability, scalable and standards compliant TV-bands administrator services.

Managing a data repository

Section 5.4 describes the various components required to manage a database repository.

Performing calculations to determine available channels

Section 5.4.6 and 5.4.7 describe the Solution's methods to calculation protected services contours and channel lists.

Registering fixed unlicensed devices

Described in Section 5.4.4

Registering licensed services not listed in the Commission's databases

Described in Section 5.4.3

How functions are performed by another entity

The Key Bridge solution does not rely on any other entities for White Space administrator functionality.

Describe data synchronization between multiple databases

Options for database synchronization are described in Section 5.4.5.

Describe how quickly this synchronization of data will be accomplished

Section 5.4.5 discusses several options for database synchronization and their speed of execution. Key Bridge supports four database synchronization options ranging from daily to near real-time.

Provide diagrams showing the architecture of the database system

See Figures 2, 3, 4, 5, 6 and 7 for high-level diagrams of the database system. Diagrams of software components and process flows are in their respective document section.

Describe how each function operates and interacts with the other functions

Sections 5 and 6 describe how the various system components interoperate and are secured.

If the entity will not perform all database functions:

Provide information on the entities operating other functions

Describe the business relationship between itself and these other entities

Address how administrator requirements are satisfied when functions are divided among multiple entities

Describe how data is transferred among entities

Describe how data is transferred among databases

Describe the schedule of such data transfers (i.e., real-time, once an hour, etc.).

The Key Bridge solution does not rely on any other entities for TV band services. Section 5.4.8 discusses how Key Bridge may provide unbundled services to other entities.

Describe the methods (e.g., interfaces, protocols) used by TV band devices to communicate with the database

Section 5.4.7 describes channel list messaging format and structure. Section 6.4 discusses message security standards, and Section 7 discusses Key Bridge resources for development, interoperability testing and device certification.

Describe procedures to verify that a device can properly communicate with the database

Section 7 discusses Key Bridge resources for development, interoperability testing and device certification.

Describe the security methods to ensure that unauthorized parties

Section 6 details this proposal's security strategy.

Cannot access the database

Sections 6.2 discusses protecting the TV bands database.

Cannot alter the database

Sections 5.4.1, 5.4.2 and 5.4.4 include discussions about data staging and verification prior to importation to the Core database.

Cannot otherwise corrupt the operation of the database system

Sections 5.2.1 and 5.2.2 discuss database clustering and high-availability, while section 6.2 discusses protecting the database.

Cannot interrupt the database system from performing its functions

Sections 5.2.1 and 5.2.2 discuss database clustering and high-availability. Section 6.2 discusses protecting the database. Section 4.4 discusses how the network architecture contributes to high-availability and resistance from attack through geographic and network diversity plus the use of 'anycast' routing.

Describe whether and how verify FCC certification of Mode I personal/portable devices

Section 5.4.1 discusses Key Bridge's equipment authorization web services, which are available to Fixed and Mode-II devices to confirm their down-stream clients are FCC certified for operation in the TV bands.

3 The Key Bridge Team's End-to-End Solution Architecture

In recent years, the computing industry has witnessed an evolution in open source, resulting in technologies that can help to meet goals for business continuity, consistent performance, and ongoing growth. Open source technologies such as Project GlassFish., the MySQL database, and the OpenSolaris operating system, offer enterprise-level features and carrier-grade reliability.

Internet service providers are increasingly adopting open source technologies to lower the cost of infrastructure, assure standards compliance and take advantage of continuous enhancement and new features by the open source community. In many instances, open source software delivers reliability and performance that meet and often exceed proprietary offerings. Open source software incorporates enhancements more quickly than proprietary technologies. When used properly, it can accelerate time-to market and expedite implementation of emerging industry standards.

The Key Bridge team combines open source software with carrier-grade servers from Oracle Inc. to create a low-cost, scalable, reliable, and flexible infrastructure for delivering future communications services. The carrier-grade solution architecture builds upon on an open source software foundation with commercial off-the-shelf (COTS) hardware technologies and support services.

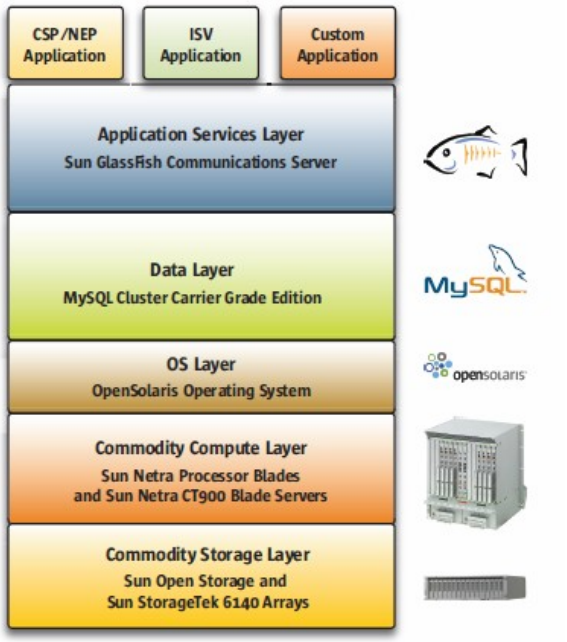


Figure 1: Key Bridge TV band database implements industry standard solution architecture for carrier-grade communication services.

3.1 A Functional System Sketch

The most basic description of the TV bands database ("Database") intended function is a channel list server. The functional block diagram in Figure 2 shows a very basic system that achieves this core function by importing and processing raw data from a number of sources, including the FCC, to calculate channel lists and respond to external inquiries.

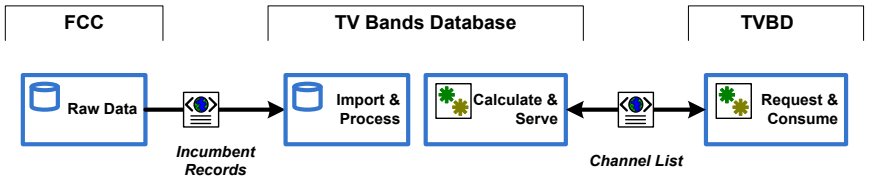


Figure 2: Basic TV bands database functional block diagram

Many additional features and functions are necessary in a real-world system that provides a channel list service, and Figure 3 illustrates the simplest schematic of the Key Bridge TV bands

database ecosystem, which incorporates all of the necessary components and communications interfaces required for an end-to-end TV bands database solution.

FCC resources and functions on the left provide for the retrieval incumbent records and equipment authorization information from several data sources, and a management web portal is necessary to accommodate oversight, reporting and enforcement requirements.

Several modules added to the TV bands database system described above support additional management capabilities, while additional communications interfaces allow convenient interaction with the database system for external systems. Woven throughout the system are security features and frameworks that assure reliable operation and communication between the database and external systems.

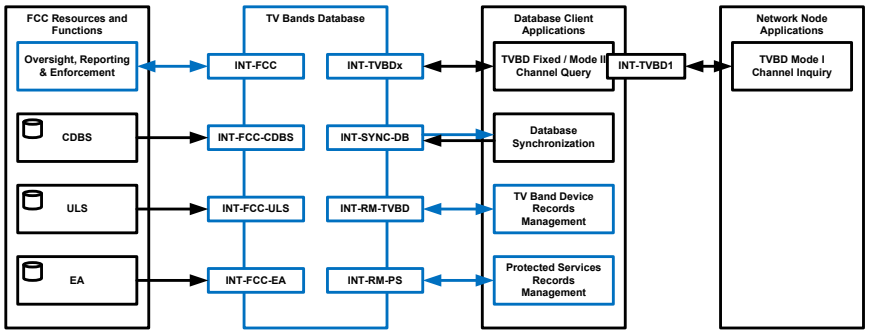


Figure 3 High-level system block diagram of the Key Bridge TV bands database ecosystem showing the four classes of participant and the logical interfaces by which they may exchange standardized information and messages.

3.2 Leveraging Industry Standards and Open Reference Architectures

The Key Bridge TV bands database solution builds upon the Sun reference architecture for Enterprise applications. It includes:

- **OpenSolaris operating system (OS)**

  Backed by world-class support from Oracle, the OpenSolaris OS provides an ideal open-source platform to develop next-generation applications. With the same robust features as the commercial Solaris 10 OS including Dynamic Tracing (DTrace) for runtime observability and performance tuning, network virtualization, and the advanced ZFS file system technology, the OpenSolaris operating system offers performance and reliability for demanding transaction workloads

- **Clustered Oracle and MySQL relational database**

  Oracle and MySQL database configurations provide a fault tolerant clustering architecture to support mission-critical applications. Designed specifically for high availability environments, these real-time, clustered databases provide a carrier grade foundation for applications that require continuous availability and dynamic on-line scalability

- **Oracle Glassfish Application Server**

  The Sun Glassfish Enterprise Server is a open source Java EE reference application server with clustering, high availability, and secure administration

- **Key Bridge TV Bands Software Portfolio**

  The Key Bridge software portfolio includes a number of modular application libraries that implement FCC rules and requirements. These modules are compiled and run within the Glassfish application server to provide TV band services with clustering, high-availability and secure administration.

When integrated together, these components and Key Bridge custom software form a comprehensive technology solution that delivers carrier-grade information service capabilities to meet the most demanding requirements of the FCC and TV bands user community.

Open source software, custom developed applications and community developed requirements contribute to a comprehensive Key Bridge TV bands database solution.

- **Event-driven architecture**

  TV band services are inherently asynchronous and event-driven. The system must efficiently respond to inquiries and events. An application server like Glassfish that fully implements the JEE Web Container is a solid foundation for creating event-driven, message-based solutions.

- **Low latency service**

  Response times must be fast and consistent, especially as services gain acceptance and demand volumes grow. Response times generally depend on subsystem processing times, and often by the speed of I/O operations and network connections. Carrier grade databases like MySQL and Oracle Clusters to minimize latencies by using main memory storage of indexes and tables to limit disk I/O (with options for storing data on high speed disks) and asynchronous operations to write log files to disk. Batching I/O operations also helps to reduce network latencies.

- **High availability infrastructure**

  TV bands infrastructure is designed to withstand hardware or software failures without resulting in a loss in service. Redundant server instances and cluster nodes allow software and hardware upgrades to occur without downtime, enhancing availability and dynamic scaling with high throughput and optimal scalability..

- **Zero downtime management**

  Application monitoring produces immediate detection of software or hardware failure, rerouting to other instances within the cluster node. System components can be taken offline for maintenance, expanded or upgraded, and brought back online without affecting service availability. An integrated backup and disaster recovery strategies also replicate data and services across geographically distributed nodes

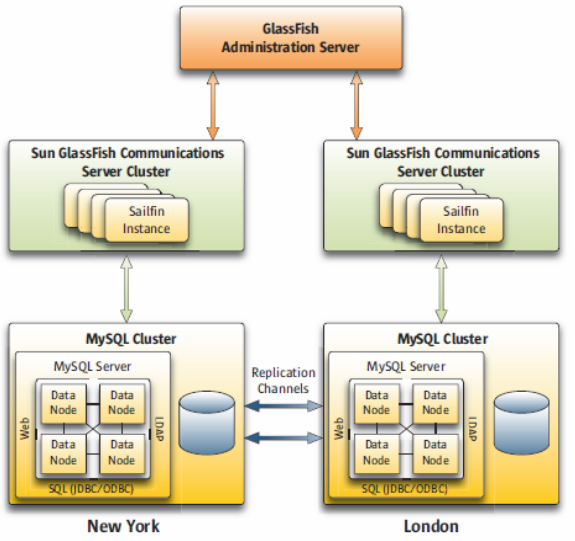


Figure 4: Example of a clustered database and application server system operating in geographically distributed facilities. The databases synchronize in real time via replication channels, and the whole system deliver always-on Web services.

3.3 Network Architecture for Distributed, High Performance Infrastructure

The Key Bridge Database solution leverages our experience designing, building and operating very large information services. Our solution provides robust, always-on information infrastructure services.

The Database system's modular design builds from an autonomous database services node ("Node"). Each Node is a self-contained hardware-software solution that provides the complete portfolio of TV band functions and services.

The complete TV bands database system incorporates four or more nodes, each supporting the others with load balancing, traffic management, backup and fail-over redundancy across physical and logically diverse installations.

The Key Bridge solution uses Level 3's High Speed IP service for Internet access. Level 3 High Speed IP service runs on one the largest and best-connected Tier 1 IP backbones in North America, and provides a scalable, fault-tolerant network with superior performance.

Each system Node only connects directly to the Internet. Nodes interconnect via a full mesh virtual network across the Internet through encrypted tunnels. Nodes employ the virtual full mesh network for application messaging, system management, automated coordination of load balancing, traffic management, internal database synchronization, plus graceful fail-over and recovery.

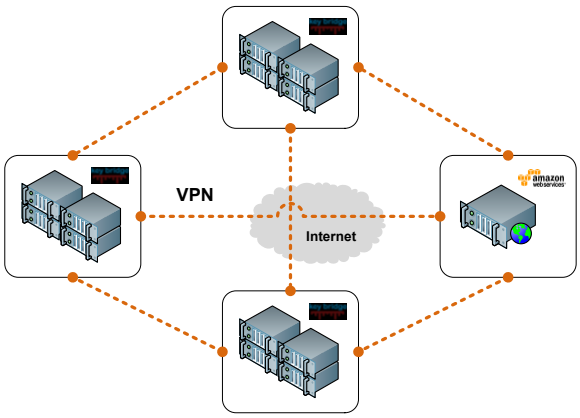


Figure 5: Virtual, private full mesh network accommodates application messaging, system management and automated coordination of load balancing and internal database synchronization

3.3.1 High Availability through Physical and Logical Redundancy

Key Bridge employs geographic and logical diversity in our distributed TV bands database system to eliminate any single points of failure. Three geographically separate installations provide physical diversity in our production system while a fourth, virtual installation, provides a failsafe backup.

To assure maximum network reach and availability, each Node connects to the Internet via two independent network access points. Network diversity enables the Key Bridge TV bands system to provide high-availability services and gracefully absorb local network outages or attacks.

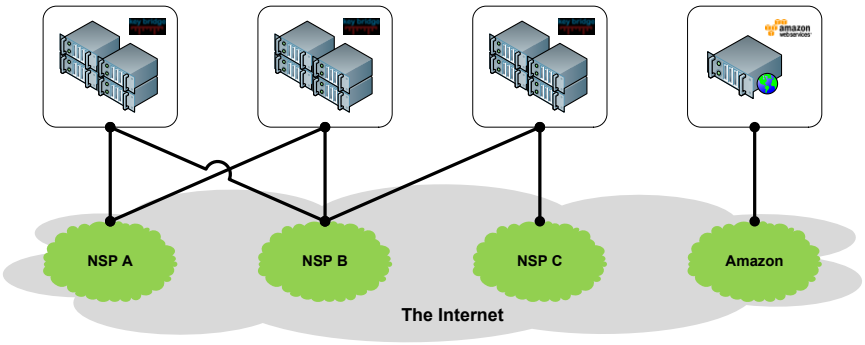


Figure 6: Key Bridge Nodes connect to the Internet via separate network service providers. Multi-homed connectivity provide greater traffic management control and reduces susceptability to denial of service attack, Internet outage or service interruption.

At each physical installation Key Bridge nodes access the Level 3 network with redundant broadband cross connects, up to 10 GigE, for unparalleled scalability and simpler management than comparable bandwidth options.

3.3.2 Improved Network Performance with Anycast

Key Bridge employs anycast routing between the three physical nodes to reach all of the TV band resources.

Anycast is a network strategy where customer connections are directed to the "nearest" or "best" destination from their location on the Internet. Anycast provides high availability and load balancing for TV band database services, which are geographically distributed over many identical servers but announced to the Internet as a single network destination.

The Key Bridge anycast strategy is similar to many domain name service strategies and several Internet root name servers, which are also computer clusters that use anycast addressing.[2]

When configured properly, anycast is highly reliable and supports automatic failover. Anycast-compatible systems, like the Key Bridge TV bands database, continuously synchronize administrative data and announce their availability directly to the network. System announcements are automatically withdrawn if a service becomes unavailable. If the service dies, the network automatically and transparently redirects incoming customer requests to the other system nodes.

[2] See IETF RFC 3258, *Distributing Authoritative Name Servers via Shared Unicast Addresses*, which describes how anycast is used for authoritative DNS services.

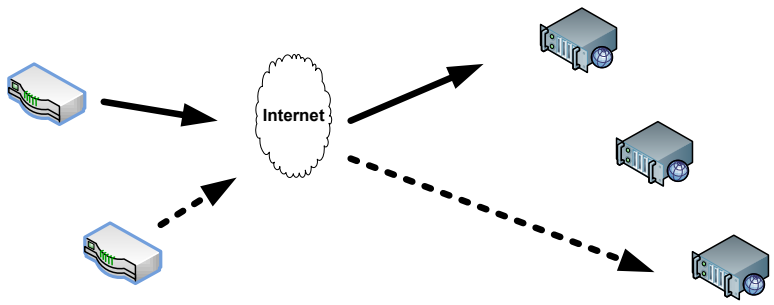


Figure 7: Anycast delivers improved network performance by routing incoming requests to the nearest available resource. In this example, two identical channel list queries are directed to different TV band nodes based on the requesting device's network location. All of the pictured nodes are announced as a single destination to the Internet (i.e. http://www.database.org).

Key Bridge also employs anycast as a security strategy to help reduce the effectiveness of distributed denial of service (DDoS) attacks. A distributed denial of service attack (DDoS) occurs when multiple systems overload the bandwidth or resources of a target system, thus making the victim's services unavailable for normal operation. With Anycast, network traffic is routed between closest nodes and incoming DDoS packets are distributed across the entire TV bands infrastructure. While this means all nodes may be affected, the net impact for any given node is a significantly attenuated attack unlikely to cause outage or interruption.

3.4 Computer Architecture

The Key Bridge Team selected the Oracle Enterprise and Web reference architecture for the TV bands database. Oracle brings more than 20 years of systems expertise and innovative thinking to systems integration and solutions architecture, their end-to-end Web solutions provide the performance, scalability, and manageability Key Bridge needs to deliver cost effective TV band services.

The Oracle Systems for Enterprise and Web reference architecture features a modular and scalable design that can start small and flexibly grow to meet changing performance and capacity requirements. Compute, storage, networks, software, and services come together in this reference architecture to deliver scalability and performance for Web environments. This integrated solution features hardware and software components extensively tested for seamless interoperability in the largest Web infrastructure deployments.

The reference architecture describes a modern Web Services solution with diverse hardware and software components options. It provides flexibility, performance, resilience and ease of use. Development and testing environments can seamlessly scale to full production by replacing low power commodity hardware with high-end computer systems, all the while running the same operating system and application frameworks.

The architecture combines components in computing, storage, networking and software into a single comprehensive solution. It provides a complete solution needed to build scalable, high-performance, and standards compliant Web services.

3.4.1 High Availability through Computer Clustering

A computer cluster is a group of linked computers, working together closely so that in many respects they form a single computer. The components of a cluster are commonly, but not always, connected to each other through fast local area networks. Clusters improve performance and availability over a single computer. High-availability (HA) clusters exploit redundancy to eliminate single points of and improve service availability by providing failover capability.

High-availability clusters have redundant computers or nodes that prevent service interruption should a system component fail. Normally when a server crashes its applications are unavailable until an operator restores service. HA clustering detects hardware/software faults and immediately remaps the visible application to a backup system without requiring administrative intervention (Failover).

Solaris Cluster is a high-availability cluster software product for the Solaris Operating System, created by Oracle Inc. It improves the availability of software services such as databases, file sharing on a network, electronic commerce websites, or other applications. Solaris Cluster operates by having redundant computers or nodes where one or more computers continue to provide service if another fails. Nodes may be located in the same data center or on different continents.

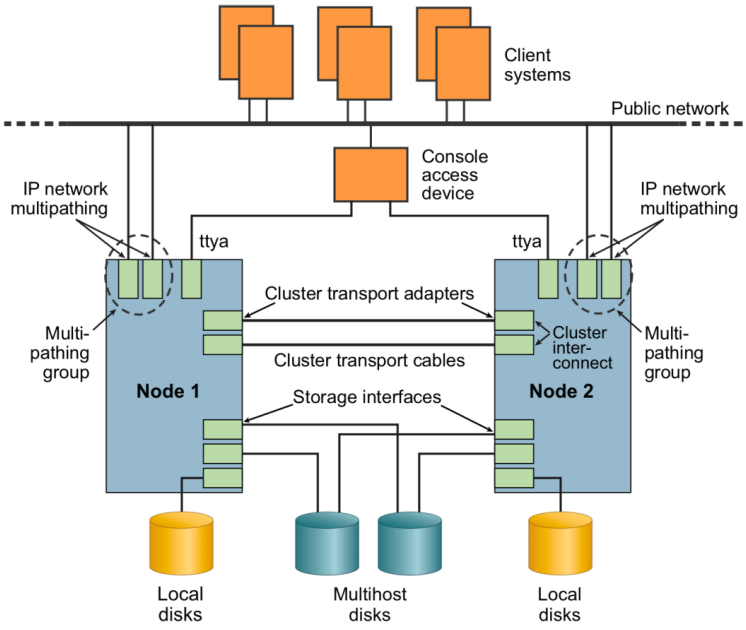


Figure 8: Solaris Cluster hardware components

A Solaris Cluster system consists of two or more servers or server domains that work together as a single entity to provide applications, system resources, and data to users. Each server generally

provides some level of redundancy. In addition, highly available, redundant disk systems support data access in the event of a service interruption on a single disk or storage subsystem. Redundant connections to the disk system assure data is not isolated in the event of a server, controller, or cable failure. A high-speed, redundant, private interconnect provides access to resources across the set of servers. Redundant connections to the public network also provide each node with multiple paths for access to outside systems, helping ensure continued access in the event of a network connection or node failure.

Each server component or node in the cluster environment contains processors, memory DIMMs, an operating system, and application software. A node consists of a domain within a server or a complete server. Key to the design of Solaris Cluster systems is the fact that no single failure in the hardware, software, interconnect, or network can cause the cluster to fail. Solaris Cluster systems prevent loss of service through hardware redundancy, hardware and software failure detection, automatic recovery of services, and failover of applications. Solaris Cluster systems also provide a single management view for all of the services in the cluster. The entire cluster appears as single Sun server, reducing the risk of errors.

Solaris Cluster systems are designed for high availability and provide the following advantages over single server solutions:

- **Increased service availability**

  Redundant resources in the cluster, coupled with the use of failover mechanisms and scalable services, can help increase application service availability

- **Increased scalability**

  Large SMP servers can be pooled together in a cluster, allowing overall capacity to be

expanded either by adding resources to the individual servers (vertical scalability) or by increasing the number of participating servers in the cluster (horizontal scalability)

- **Better resource utilization**

  Load balancing and cluster-wide resource management promotes sharing of system resources across multiple application services and allows system resources to be reassigned to other services instead of sitting idle

- **Improved manageability**

  A single management environment for the cluster offers the opportunity to manage components, services, and resources holistically to help improve efficiency and drive down costs

3.4.2 Performance Management with Load Balancing

Load-balancing may occur when multiple computers are linked together to share computational workload or function as a single virtual computer. Logically, from the user side, they are multiple machines, but function as a single virtual machine. Requests initiated from the user are managed by, and distributed among, all the standalone computers to form a cluster. This results in balanced computational work among different machines, improving the performance of the cluster system.

In computer networking, load balancing is a technique to distribute workload evenly across two or more computers, network links, CPUs, hard drives, or other resources, in order to get optimal resource utilization, maximize throughput, minimize response time, and avoid overload. Using multiple components with load balancing, instead of a single component, may increase reliability through redundancy. The load balancing service is usually provided by a dedicated program or hardware device (such as a multilayer switch or a DNS server).

It is commonly used to mediate internal communications in computer clusters, especially high-availability clusters.

Load balancing is often used to implement failover — the continuation of a service after the failure of one or more of its components. The components are monitored continually (e.g., web servers may be monitored by fetching known pages), and when one becomes non-responsive, the load balancer is informed and no longer sends traffic to it. And when a component comes back on line, the load balancer begins to route traffic to it again. For this to work there must be at least one component in excess of the service's capacity. This is much less expensive and more flexible than failover approaches where a single "live" component is paired with a single "backup" component that takes over in the event of a failure. In a RAID disk controller, using RAID1 (mirroring) is analogous to the "live/backup" approach to failover, where RAID5 analogous to load balancing failover.

3.5 A Modular Software Architecture for Flexible Web Services

The Key Bridge TV bands solution implements industry best practice for the development and operation of database applications. We adopt a modular software strategy and implement the Java Platform, Enterprise Edition (Java EE) reference architecture. Application development, testing, integration and operation follow the Java EE recommended practice.

3.5.1 System Analysis: High Level Business Processes and Workflow

Web service application modules must they work together smoothly. It is important to understand the application’s requirements from at a high level, business perspective. Once outlined, each module application’s functions and interactions are clear and the application architecture can be addressed.

Recall that the first function the TV bands system provides to customers is a list of available channels based on their location and type of device. Other functions, like registration, synchronization, oversight and records verification, are supporting management requirements for the channel list function. To request a channel list from the service, TV band devices submit their identifying information and geographic location from an embedded software application. Building a channel list includes determining whether the device is FCC certified, whether it has a commercial account in good standing, and analyzing the protected status of nearby incumbent transmitter sites. After calculating a channel list, the server assembles a formatted, machine-readable message. The TV bands system logs the transaction and, if applicable, submits an event detail record for payment.

In essence, the TV bands enterprise system consists of a front-end customer Web portal and Web service, which provides a face to its customers, and a back-end workflow manager, which handles the sub-system integration.

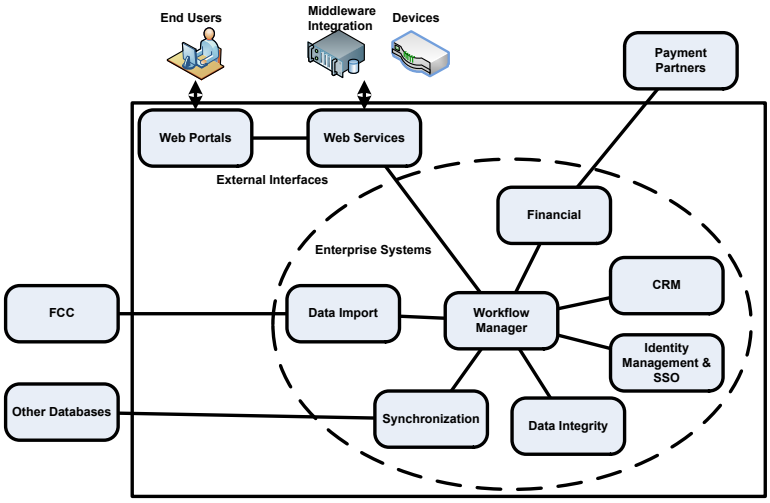


Figure 9: TV Bands enterprise system logical communications structure, illustrating how functional blocks communicate and interoperate.

As shown in Figure 9, there are four categories of external party that interact with the TV bands business process:

1. Customers use the TV bands Web to register devices and manage their commercial accounts. They review incumbent records and run business intelligence reports against the database. Customers expect to have certain services available to them, such as the ability to track status and receive e-mails about status changes. Customers use Web browsers to access Web portals and standards-compliant software to access Web services.
2. The FCC provides a data feed of incumbent records. These are provided en-bulk for file transfer by FTP or HTTP.
3. Other Database system administrators must synchronize their databases, and a publish/subscribe method is shown
4. External payment processors clear retail payments for registration and possible transaction fees.

The workflow manager is at the heart of the TV bands enterprise system, responsible for coordinating all activities necessary to respond to a customer inquiry or instruction. It interacts with:

- The customer Web site to handle Customer matters like registration, records review and oversight.
- A credit card service to collect payment
- A data integrity service to ensure that records written to the database are properly formatted and complete
- A data import and synchronization service to ensure the database remains up-to-date.

- A customer relationship management service to handle customer accounts, service and status

Figure 10 shows the channel list workflow. When it receives an inquiry for a channel list from a TV band device, the workflow manager writes a query log. Before proceeding, it verifies that the device is authorized by the FCC to receive channel lists (is certified and not on a blacklist) and that is has an active commercial account with available funds or credit for the transaction fee. If not, workflow manager cancels the request, notifies the customer, and ends. Otherwise, it proceeds to fulfill the request, which entails checking the geographic service contours for each class of protected entity in the database. The workflow manager then embeds the complete, valid channel list into a standards-compliant message format. The message is then encrypted, signed, and sent to the requesting device. In a production system the entire process takes less than a second to execute.

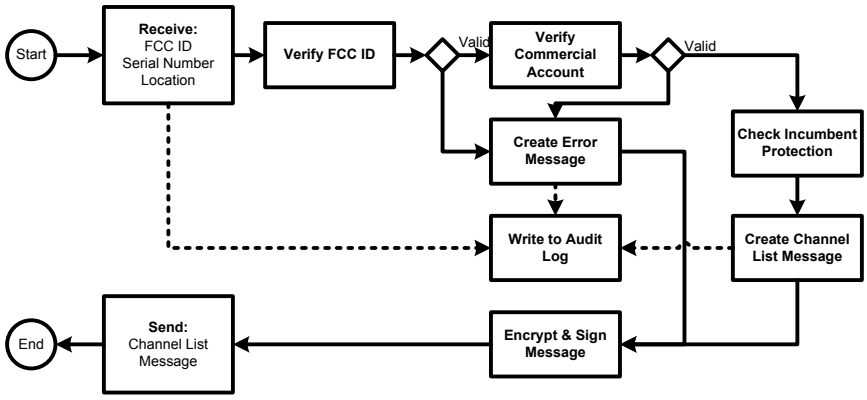


Figure 10: Channel list business logic and work flow. Note the rich logging trail for information reporting, quality control and oversight.

The process begins when a TV band device submits its location and identification to a channel list Web service. When which happens, the workflow manager provides other services as necessary to handle the request.

- The equipment authorization is confirmed both for device type certification and FCC black list
- The device's commercial account status is confirmed
- Geographic service contours are analyzed for each class of incumbent service
- A channel list is constructed, encrypted and sent back to the requestor

3.5.2 Building on the Java Enterprise Edition Framework

Java EE is an industry standard software platform for server programming in the Java programming language. The Java platform (Enterprise Edition) includes libraries that support fault-tolerant, distributed, multi-tier Java software based on modular components running on an application server.

J2EE, Sun's implementation of Java EE, provides server-side and client-side support for enterprise, multitier applications. Client tier applications provide the user interface, middle-tier modules provide client services and business logic, and backend enterprise information systems providing data management.

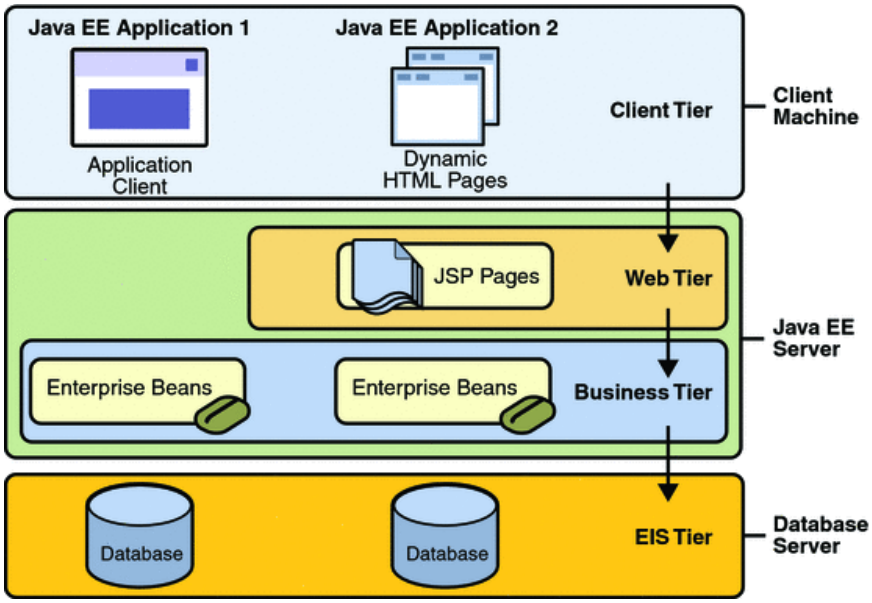


Figure 11: the various components and services that make up a typical Java EE (J2EE) environment

A multitier distributed application runs on different devices. The J2EE architecture defines a client tier, a middle tier, and a backend tier providing services of existing information systems. J2EE supports a variety of client types outside and inside the firewall. The middle tier supports client services through Web containers and business-logic component services through the Enterprise JavaBeans™ (EJBTM) containers. The enterprise information system (EIS) tier supports access and integration of relational databases and other information systems.

Java EE containers are standardized runtime environments that provide component services for applications. Components can use these resources on any J2EE platform. For example, J2EE Web containers provide runtime support for responding to client requests, performing request time processing (such as invoking JSP or servlet behavior), and returning results to the client. All EJB containers provide automated support for transaction and life cycle management of EJB components, as well as component lookup and other services. Containers also provide

standardized access to enterprise information systems; for example, providing RDBMS access through the JDBC API.

The J2EE client tier provides support for a variety of client types including static and dynamic HTML pages within a Web portal or stand-alone Java language applications. J2EE clients access the middle tier using open Web communication standards like HTTP, HTTPS, HTML, and XML.

The Java EE standard and software framework describes several application execution environments, or Containers. These provide pre-configured and tested sets of common software modules developers use to build their own application. Java EE application containers and associated software modules help assure standards-compliant applications and simplify the software development process. They also streamline interoperability testing and certification.

3.5.2.1 Functional Interoperability with Java Containers

There are four major application execution environments, called Java EE Containers. These listed below and illustrated in Figure 12.

- **Applet Container**

  Applets are small Java applications designed to run within a web browser. Applets use resources of and are restricted to the security framework in the web browser.

- **Application Client Container**

  Standalone applications developed within the Application Client Container enjoy streamlined interaction with Web Container resources. Clients run on hardware ranging from powerful desktop machines to tiny consumer electronic devices. They provide a browser-based or stand-alone interface and can communicate with, and use services

provided by, one or more Middle Tiers container. Clients support internationalization and a variety of development environments and languages.

- **Web Container**

  A Web container is a runtime environment for a Web application; a Web application runs within a Web container of a Web server. A Web container provides Web components with a naming context and life cycle management. Web servers also provide services such as security, concurrency, transactions, and swapping to secondary storage. A Web server need not be located on the same machine as the EJB server. In some cases, a Web container may communicate with other Web containers. Web services and Web portals run within the Web Container, which provides a comprehensive framework for creating scalable, standards-compliant Web-based application. Web containers run servlets, which are programs that extends the functionality of a Web server. Servlets receive a request from a client, dynamically generate the response (possibly querying databases to fulfill the request), and then send the response containing an HTML or XML document to the client.

- **EJB Container**

  Enterprise Java Bean Container is a generic middleware application server, providing support for network resources and service oriented architecture.

Figure 12 illustrates the Java EE reference architecture. Containers include different sets of standard software modules and communicate via standard methods. Java EE provides seamless database integration at all possible levels.

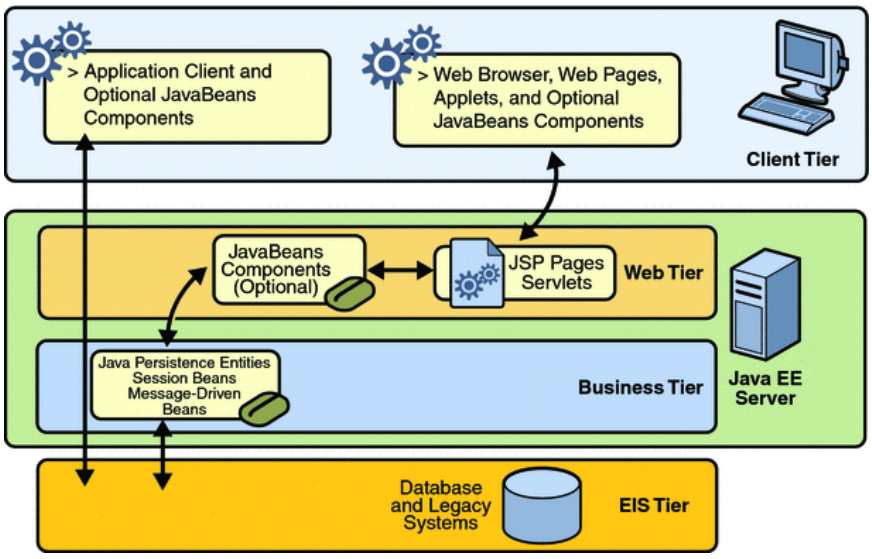


Figure 12: Java EE Framework reference architecture showing standard software modules and defined methods of interoperation.

3.5.3 Overview of Web Services and SOA

Web services are Web based applications that use open, XML-based standards and transport protocols to exchange data with clients.

Web services build on a set of XML-based open standards, such as the Web Services Description Language (WSDL), the Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI). These standards provide a common and interoperable approach for defining, publishing, and using web services. Figure 1 illustrates how the Java APIs for XML Registries (JAXR) and Java APIs for XML Remote Procedure Calls (JAX-RPC) play a role in publishing, discovering, and using web services.

Figure 13: The Java EE Publish-Discover-Invoke model

From a software developer's perspective, a web service is a service-oriented architecture and collection of services that communicate with each other (and end-user clients) through well-defined interfaces. One advantage of service-oriented architecture is that it allows the development of loosely coupled applications that can be distributed and accessed, from any client, across the network.

3.5.4 Simplified Interoperability with Modular Programming

Modular Programming is a development model where a software application is composed of separate parts, called modules. Modular development enforces a separation and isolation of discrete functional blocks and serves to improve maintainability by enforcing logical boundaries between components. Benefits of Modular Programming include the isolation of functional blocks such that none or only a few modules depend upon other modules of the application. In comparison with a Monolithic application where the smallest component is the entire application itself, Modular development more easily supports software reusability, unit testing, and distributed development teams.

Theoretically, in modular software project development no single team or team member creates the whole system or needs to even know about the system as a whole. Rather, individuals and teams can focus their assigned tasks.

The main application incorporates modules through interfaces. A software interface describes the services provided and inputs required by the respective module.

Modular software components are the building blocks for service orientation throughout software engineering. Examples include Web Services and Service-Oriented Architecture (SOA) - whereby a software component is converted into a service and made available to other computer modules via a standard service definition.

Service-Oriented Architecture attempts to package software functionality as interoperable services. Rather than defining an API, SOA defines the interface in terms of protocols and functionality. Service-orientation separates modular software functions into distinct units, or services, and enables developers to publish them over a network as a web service. Service subscribers may combine and reuse them in the production of applications.

SOA requires that service descriptions, metadata, provide sufficient detail to describe service characteristics and the data they consumer and produce. The Web Services Description Language (WSDL) typically describe the services themselves, while the SOAP or REST frameworks typically describes the communications protocols.

Web services support interoperable machine-to-machine communications over a network. A Web service has an interface described in a standard machine-readable format (Web Services Description Language WSDL). Other software systems may interact with web services in a manner prescribed by its description and typically use XML over HTTP.

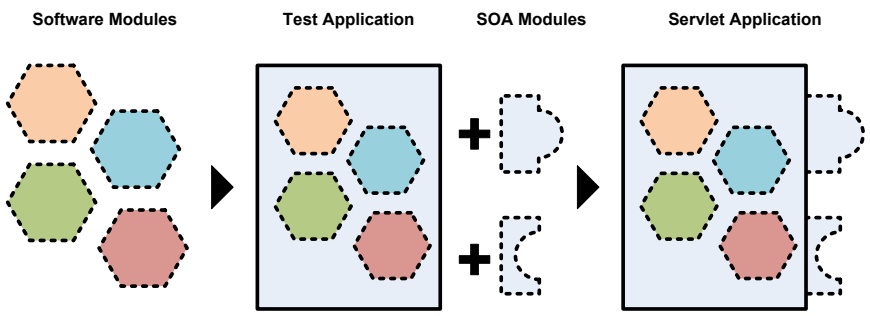


Figure 14: Illustration of the modular development process, whereby functionally independent software modules are compiled into a test application for testing, then compiled with SOA modules to create a Servlet application.

Software developers create Internet web services using the Java Servlet API to run within a Java EE Web Container. Servlets are a standards-based application-programming interface for creating SOA applications that respond to SOAP and REST compatible requests.

As described above, development begins with a group of functionally independent software modules. During development, modules are often mixed and matched into test applications to confirm their proper functionality. A Servlet application is created by adding SOA modules, which assure the program will send and receive standards-compliant formatted messages. This process is illustrated in Figure 14.

Java Servlets are deployed and executed within a Application Server. Application Servers are instances of a Web Container, itself a Java applications that provide for the efficient execution and standardization of function-specific programs that share common requirements like networking, web services interfaces, file system access and database connectors.

Once compiled into a Servlet, the application server presents the complete set of modules as a web service. This concept is illustrated in Figure 15.

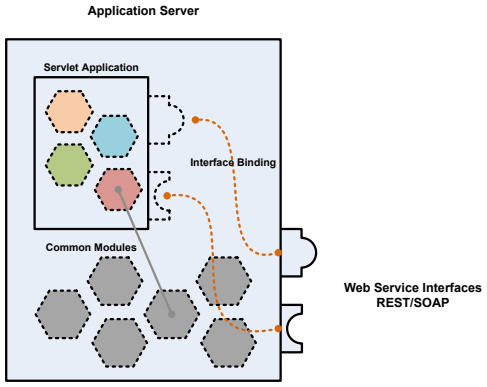


Figure 15: A web services modular software architecture, where the Servlet application is deployed inside an Application server. The Servlet's send and receive capabilities are exposed by the application server as web services interfaces.

4 Methods and Products in our Technical Implementation

The Key Bridge Team's software integration strategy is to leverage best practice and product wherever possible to deliver an enterprise quality TV bands database system. Accordingly, we have designed an end-to-end solution that includes the most robust commercial quality software available. From operating system to file storage, data encryption and database applications, the Key Bridge TV bands solution is built, most robust and highest performance software systems available today, all backed by the full commercial support and maintenance capabilities of their respective companies.

The Key Bridge solution makes extensive use of modular software components and application server frameworks. By this method our web services system inherently robust and easily scalable while preserving flexibility in deployment and software that is straightforward to maintain, modify and improve as new feature are requirements.

The TV bands database ecosystem illustrated in Figure 16 consists of three basic classes of computer system, integrated into a single end-to-end solution via an Enterprise Service Bus. These sub-systems are:

1. A relational database
2. An application server, and
3. An end-user client

The Database system is a native database application running directly on the operating system. The database application responds to standard SQL commands via its own proprietary database interfaces.

The Web Services system is an application server that itself is a Java application and provides a common operational framework for other Java applications.

In our system, the application server is responsible for establishing and managing database connectors. Access to the database is pooled, load balanced and wrapped in a basic security framework before being presented to server applications as a standards compliant database connector. By this method server, applications are isolated from the proprietary communications protocols of the database. They may thus be developed and tested as software modules against any brand of database and may employ standards based database access methods.

The end user application can be native or written in Java. The only requirements placed on the end user application are they must support web services, protocols and open standards like HTTP and XML. For testing and development purposes Key Bridge has release a developer library, API and client application sample code.

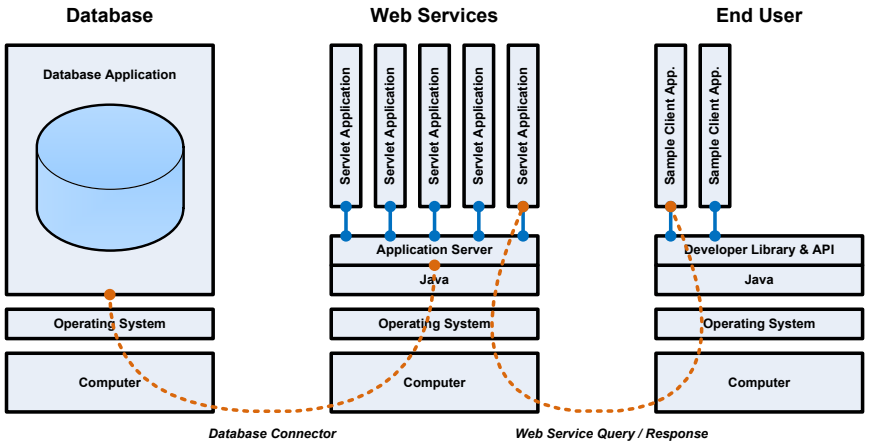


Figure 16: Computer and Software Architecture showing how client applications communicate with server applications, which in turn execute prescribed transactions with the database application via a connector provided through an application server. Neither the client nor the server application directly accesses the database.

In summary: End user applications communicate with Servlet applications, expressed as web services via an Application server. Servlet applications may access the database via connectors, which the Application server also establishes and manages.

4.1 Standardization with Software Application Frameworks

Key Bridge builds upon a suite of standards-based, open, extensible software provided by Oracle Inc. to develop information infrastructures using a service-oriented architecture approach. This unified and comprehensive software solution delivers secure, robust and scalable TV bands database solution in a flexible SOA environment based on open standards a communications protocols.

Oracle is a leading provider of open-source software with unmatched experience developing communities, integrating software and supporting products. Sun helps companies around the world reduce the cost and risk in development of applications through their deployment.

Application & Integration Software is the heart of any Service-Oriented Architecture (SOA). Sun Java Composite Application Platform Suite and Sun GlassFish Enterprise Server provide a highly scalable and reliable platform for the standards-based deployment of Java applications and Web services. Sun offerings are used organizations and enterprises that require a solid services-based foundation.

Commercial software products and technologies incorporated the Key Bridge TV bands solution includes:

- Sun GlassFish Enterprise Service Bus
- Sun GlassFish Enterprise Server
- Sun GlassFish Message Queue

- Sun Java System Directory Server
- Sun OpenSSO Access Management

4.1.1 Web Container: The GlassFish Enterprise Server

The Oracle GlassFish Enterprise Server is the leading open-source and open community platform for building and deploying next-generation applications and services. Java Platform, Enterprise Edition (Java EE) is the industry standard for implementing enterprise-class service-oriented architecture (SOA) and next-generation web applications.

Built on the open-source Project GlassFish, the Oracle GlassFish Enterprise Server delivers a costefficient, enterprise-class application server for demanding enterprise and Web 2.0 applications. It delivers best-in-class performance and enterprise features at a fraction of the cost of proprietary application servers.

GlassFish Enterprise Server is the Java™ Platform, Enterprise Edition (Java EE platform) reference implementation and the first application server to support Java EE 5 technology, which delivers ready access to a secure, portable and scalable platform for enterprise applications.

With support for centralized administration and high-availability clustering, GlassFish Enterprise Server is built for business-critical environments where centralized management is key to lowering operations costs.

4.1.1.1 High availability

GlassFish Enterprise Server supports application clusters for scalability and high availability. Application clusters can be created dynamically and adjusted on the fly to meet user demand without service interruption. For deployments that must handle application server failure without service interruption, in-memory session replication is a robust and easy-to-use solution. For deployments that require 99.999% availability with no loss of session data, GlassFish Enterprise Server leverages the High Availability Database (HADB), which helps ensure data integrity and availability.

- Create and manage clusters from a single administration console and manage a cluster as a single entity
- Dynamically grow or shrink a cluster by adding or removing application server instances
- Load-balancing plug-in monitors cluster health and balances load across available instances

4.1.1.2 Performance

GlassFish Enterprise Server is the only open-source application server to post a SPECjAppServer 2004 result. (This industrydefined benchmark documents Java EE application server performance.)

- GlassFish is the fastest open-source application server, surpassing the industry's leading application servers
- GlassFish is highly scalable and optimized for multi-core servers, including Sun servers with CoolThreads technology
- Fast Infoset support improves Web services performance by a magnitude of 2x to 4x, with Oracle’s Project Metro JAX-WS surpassing other implementations

4.1.1.3 Service-Oriented Architecture (SOA)

With strong support for Open ESB, an open source project created from Oracle's award-winning Java Composite Application Suite (Java CAPS), which enables enterprises to build flexible SOA architectures; Project Metro; RESTful Web services; and Web services management, GlassFish Enterprise Server is an ideal platform for SOA applications.

GlassFish Enterprise Server supports GlassFish ESB for easy integration of Web services and existing enterprise resources to create loosely coupled, enterprise-class composite applications. Web services are first-class manageable objects when deployed to GlassFish Enterprise Server; Web services can be automatically discovered, managed and monitored. If monitoring is enabled for a Web services endpoint, information about response time, throughput, requests, and faults is collected and viewed through the administration console, along with Simple Object Access Protocol (SOAP) or Representational State Transfer (REST) message content. Also, Web services testing pages can be automatically generated, eliminating the need for explicit Web services client development.

4.1.1.4 Database Interoperability

The GlassFish Application Server supports connectivity to any database management system with a corresponding J2EE certified JDBC driver, including:

- Oracle
- Sybase
- Microsoft SQL Server
- IBM DB2
- MySQL

- Postgres
- Java DB

4.1.2 User Account Management with Java System Directory Server

Key Bridge employs the Oracle Java System Directory Server for user account management and resource privilege management. Sun Java System Directory Server is the only high-performance directory server with incorporated data services including proxy, virtual directory and data distribution to provide a highly available directory service in one solution.

Directory Server implements a wide range of Lightweight Directory Access Protocol (LDAP) and related standards, including full compliance with LDAPv3 but also support for Directory Service Markup Language (DSMLv2). It also offers multi-master replication, access control, and many extensions.

Key features include

- Comprehensive, high-performance directory solution Features 64-bit enterprise-class directory for sustained search performance and near-relational database write performance
- Includes virtual directory and directory proxy services
- Seamless, nonintrusive integration with Microsoft Active Directory
- Built for maximum availability and massive scalability
- Delivers a highly-flexible replication environment to help ensure data availability

- Provides for vertical and horizontal growth with linear CPU scalability to 18 CPUs
- Industry-leading security and access control Robust security with data and communication encryption and password protection
- Secures data and minimizes risk with Access Control Instructions (ACIs) at the attribute and proxy level

Secure, simplified access to the entire portfolio of Key Bridge services is enabled with the Java System Directory Server and Single Sign-On working together.

4.1.3 User Account Management and Security with Single Sign-On

Key Bridge employs Oracle's comprehensive Single Sign-On (SSO) solution, OpenSSO, to enable secure Web access management, including centralized SSO and security policy for Web Applications and Web services. Key Bridge employs OpenSSO for user account management and secure access to Web applications and services.

OpenSSO is an open-source access management platform. It enables Single Sign-On (SSO) capabilities for web services. OpenSSO is an integration solution for Web access management, federation, and Web services security. It is the first integrated solution for managing Single-Sign-On, authorization, and personalization in Web, federated, and Web services environments.

Using Sun OpenSSO Enterprise, Key Bridge centralizes and enforces SSO and security policy for Web applications and Services in a repeatable, scalable manner. This reduces account related security risks. Sun OpenSSO Enterprise enables:

- Configure agents and servers to establish resource security and access policies from a single, centralized console
- Secure applications and provide them with Single Sign-On capability
- Enforce XACML-based policy management, a standards based framework for defining and enforcing policy across an enterprise

4.2 Relational Database Management Systems

The Key Bridge solution employs several relational database instances for the storage and processing of information. Our core, production system is built on a Oracle Enterprise system, whereas our feeder, distribution and development systems employ the MySQL database.

4.2.1 The TV Bands Core Database is Oracle

The main TV bands database is Oracle. Sun and Oracle have worked together for over two decades to make Solaris a highly optimized database and application deployment platform, ideal for Oracle Applications and over 10,000 other software packages.

Oracle Database Enterprise Edition delivers industry leading performance, scalability, security and reliability on a choice of clustered or single-servers. It provides comprehensive features to easily manage the most demanding transaction processing, business intelligence, and content management applications.

Exadata, the Oracle Database Machine is the world's fastest for any type of database workload, and the only database machine that runs transaction processing applications. It is a complete

package of software, servers, storage and networking for all data management, including data warehousing, transaction processing and consolidated mixed application workloads.

At the heart of this system is the Oracle Exadata Storage Server, which has smart storage software built in. The smart storage software offloads data-intensive query processing from Oracle Database 11g servers and brings it closer to the data. As a result, much less data travels over the server's fast InfiniBand interconnects—dramatically improving both query performance and concurrency for transaction processing and data warehousing applications.

4.2.1.1 Oracle High Availability Clusters

Oracle Real Application Clusters (Oracle RAC) enables a single database to run across a cluster of servers, providing unbeatable fault tolerance, performance, and scalability with no application changes necessary. Benefits of Oracle clustering include:

- 24/7 availability: Provides continuous uptime for database applications
- On-demand scalability: Expands capacity by simply adding servers to your cluster
- World-record performance: Runs faster than the fastest mainframe

Oracle Real Application Clusters (RAC) provides unbeatable fault tolerance, performance and scalability. Oracle RAC is a cluster database with a shared cache architecture that provides a highly scale and available database solution across a cluster of servers, providing fault tolerance from hardware failures or planned outages.

Oracle RAC offers features in the following areas:

- Scalability
- Availability
- Load balancing

- Failover

Oracle RAC provides very high availability for applications by removing the single point of failure with a single server. If a node in the cluster fails or must be removed for maintenance, the Oracle Database continues running on the remaining nodes. Individual nodes may be shut down for maintenance without affecting the overall functionality of the system.

When a system is repaired and ready to rejoin the cluster, Oracle's Fast Application Notification enables end-to-end recovery of applications and load balancing.

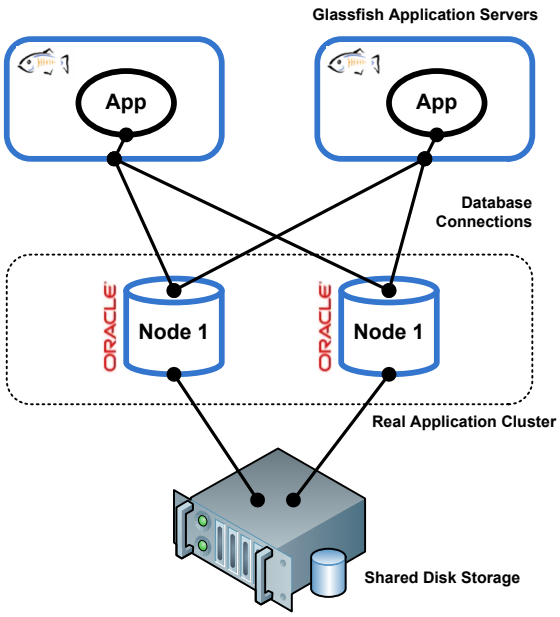


Figure 17: Oracle Real Application Clusters (RAC) provides fault tolerance, performance and scalability. Application servers connect to redundant nodes within the cluster. The process is transparent to applications and users.

4.2.1.2 Oracle Performance

Oracle clusters are from standardized, commodity computers and storage. When more processing power is required, additional servers may be added without interrupting operation of the Database. Database administrators may manage and control individual application workloads.

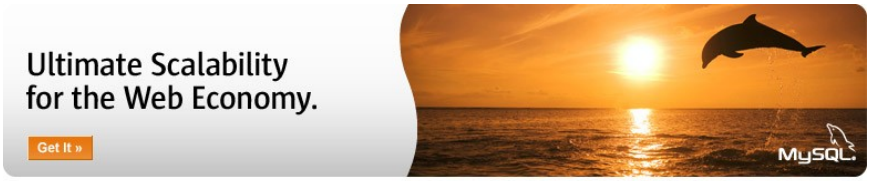
4.2.1.3 Oracle Advanced Security

Oracle Advanced Security, part of Oracle's comprehensive portfolio of database security solutions, helps organizations comply with privacy and regulatory mandates such as Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), as well as numerous breach notification laws. With Oracle Advanced Security, customers can transparently encrypt all application data or specific sensitive columns, such as credit cards, social security numbers, or personally identifiable information (PII). By encrypting data at rest in the database as well as whenever it leaves the database over the network or via backups, Oracle Advanced Security provides the most cost-effective solution for comprehensive data protection.

Benefits of using Oracle Advanced security to protect commercially sensitive data include:

- Protect all application data quickly and easily: Encrypt the entire table space or specific sensitive columns without making any changes to existing applications.
- Transparent encryption for Oracle database traffic, disk backups, and exports.
- Leverage secure, built-in key management and integration
- Support for PKI, Kerberos and RADIUS-based strong authentication and identity assurance

4.2.2 The TV Bands Non-Core Database Instances are MySQL



MySQL database is the world's most popular open source database. It provides fast performance, high reliability and ease of use. MySQL Enterprise Server software is the most reliable, secure and up-to-date version of MySQL for cost-effectively delivering E-commerce, Online Transaction Processing (OLTP), and multi-terabyte Data Warehousing applications. It is a fully integrated transaction-safe, ACID compliant database with full commit, rollback, crash recovery and row level locking capabilities. MySQL delivers the ease of use, scalability, and performance that has made MySQL the world's most popular open source database.

4.2.2.1 High Availability with MySQL clustering

MySQL Cluster is a high availability relational database with a “shared-nothing” distributed and no single point of failure. It routinely provides 99.999% availability and meets the most demanding mission-critical application requirements.

MySQL Cluster is widely adopted by the telecommunications and Internet services community. It provides carrier subscriber database applications (ie HLR/HSS) as well as the data layer in SDPs, Value-Added Services and Call Control.

MySQL Cluster's real-time design delivers predictable, millisecond response times with the ability to service tens of thousands of transactions per second. Support for in-memory and disk based data, automatic data partitioning with load balancing and the ability to add nodes to a

running cluster with zero downtime allows linear database scalability to handle the most unpredictable workloads.

Reliability and constant availability are hallmarks of MySQL, with customers relying on MySQL to guarantee around-the-clock uptime. MySQL offers a variety of high-availability options from high-speed master/slave replication configurations, to specialized Cluster servers offering instant failover, to third party vendors offering unique high-availability solutions for the MySQL database server.

4.2.2.2 MySQL Scability and Flexibility

The MySQL database server provides the ultimate in scalability, sporting the capacity to handle deeply embedded applications with a footprint of only 1MB to running massive data warehouses holding terabytes of information. Platform flexibility is a stalwart feature of MySQL with all flavors of Linux, UNIX, and Windows being supported. And, of course, the open source nature of MySQL allows complete customization for those wanting to add unique requirements to the database server.

A unique storage-engine architecture allows database professionals to configure the MySQL database server specifically for particular applications, with the end result being amazing performance results. Whether the intended application is a high-speed transactional processing system or a high-volume web site that services a billion queries a day, MySQL can meet the most demanding performance expectations of any system. With high-speed load utilities, distinctive memory caches, full text indexes, and other performance-enhancing mechanisms, MySQL offers all the right ammunition for today's critical business systems.

4.2.2.3 MySQL Database with Solaris Cluster

MySQL delivers high performance and reliability while keeping costs low by eliminating licensing fees. Solaris Cluster is an integrated hardware and software environment that creates highly available data services. The primary advantage of deploying the MySQL database in a Solaris Cluster environment is high availability. The Solaris Cluster environment provides fault monitoring and failover capabilities not only for the MySQL software, but also for the entire infrastructure including servers, storage, interconnects, and the operating system. If any component of the entire infrastructure fails, that failure is isolated and managed independently with no impact on availability.

MySQL Master-Slave configurations, deployed outside of a Solaris Cluster environment, provide limited availability: if the master fails, then the slave can manually be assigned master status and take over operation. However, this process is not automatic but requires manual intervention by a system administrator. Solaris Cluster removes this limitation, as it automatically fails over in the case of a master node failure. In addition, Solaris Cluster provides high availability for slaves as well as for masters. By providing high availability for slaves, these slaves can be kept updated with the masters throughout database transactions, thereby supporting scalability of MySQL database services. The Solaris cluster also provides both failover and scalable Apache Web server instances, thereby offering larger high availability coverage of the SAMP stack. Thus, MySQL Master-Slave configurations deployed in Solaris Cluster environment become highly available in the true sense.

Solaris Cluster deployments provide additional benefits beyond high availability. The Solaris Cluster environment can simplify administration by enabling clustered systems to be managed as if they were a single system. Data services, such as the MySQL database, can be deployed in

Solaris Containers, providing the benefits of consolidation (as provided by Solaris Containers) as well as high availability (as provided by Solaris Cluster). Finally, both the MySQL database and Solaris Cluster are free and open source software, helping to contain costs and provide a low-cost solution for highly available databases.

4.3 Assured Identity and Authentication with Digital Certificates and Public Key Infrastructure (PKI)

Key Bridge has partnered with Symantec to provide signed digital certificates and a robust, globally deployed public key infrastructure (PKI) suitable for all authentication and encryption requirements.

4.4 Device Certificate Services

Digital certificates embedded into hardware devices enable service providers to authenticate remote devices before allowing access to networks and services.

Symantec Device Certificate Services is a high-volume, high-performance batch issuance certificate service that provides a fast, efficient, and cost-effective way to embed X.509 certificates into any type of hardware device during the manufacturing process. The X.509 certificate allows service providers to perform strong authentication of distributed hardware and prevent unauthorized or cloned devices from obtaining access.

How Device Certificate Issuance Works

1. Device manufacturers order certificates in bulk by providing Key Bridge / Symantec with a list of MAC addresses, unique device IDs for the certificates or by providing a standard PKCS10 Certificate Signing Request.

2. Key Bridge / Symantec securely return the issued certificates and private keys, if requested, to the manufacturers in an encrypted format.
3. The manufacturer embeds the certificates during the device manufacturing process.

The Key Bridge / Symantec turnkey solution generates batches of digital certificates and private keys through an easy-to-use Web interface without the technical investment. This base platform is highly flexible and can be configured for specific industry needs.

4.4.1 A useful example from the WiMAX™ Industry

Symantec supports the WiMAX Forum® requirement for mutual authentication of devices and authentication servers using X.509-standard digital certificates. The WiMAX Forum selected Symantec as the sole provider for its Server PKI for service providers. Symantec was also chosen to provide PKI certificates to WiMAX Device Manufacturers.

4.5 Managed PKI Service

The Key Bridge / Symantec offered PKI solution leads the industry with trusted PKI solutions that reduce the complexity of securing today's mission-critical interactions. With PKI solutions, Symantec provides the unmatched flexibility and scalability that global enterprises as well as regional, federal, and international governments need to meet a broad range of business and operational requirements.

The Key Bridge / Symantec Managed PKI Service is a PKI certificate management and authentication service that runs on VeriSign's proven, globally managed, highly reliable infrastructure. Quick to deploy and easily integrated into the existing network infrastructure, Managed PKI Service is optimized for heterogeneous operating system environments,

homogeneous Windows and Active Directory environments, and non-PC based devices such as ATMs, printers, telecommunications, and, as relevant to this proposal, TV band devices.

Key Bridge / Symantec Managed PKI is the premier technology that provides all of the essential security services needed for establishing trust in online electronic transactions that require confidentiality, integrity, identity authentication and non-repudiation.

- Real-time issuance to customers, business partners, Web services applications and network devices
- Full lifecycle management to issue, renew, revoke, and manage digital certificates with maximum flexibility
- Automated enrollment for users, servers, applications, network devices
- Standards-based digital certificates can be installed on open standards authentication devices with native PKI support: computers, tokens, smartcards, mobile phones, and more
- Simplified Middleware provides an easy-to-use tool for renewal and application integration
- Validation of certificates through the highly available, secure Key Bridge / Symantec infrastructure with daily updated Certificate Revocation Lists (CRLs)
- Audited policies and procedures to meet the most rigorous compliance requirements

Advantages that the Key Bridge / Symantec end-to-end embedded certificate and PKI solution include:

- Symantec operates the longest running commercial PKI platform in the world and has issued more than 103 million device certificates

- Each year, Symantec issues 42,300 Class 1 certificates, more than 16,000 ECA certificates.
- 11,500 secure online transactions are enabled every second by Symantec

4.6 Key Bridge Custom TV Bands Software

Key Bridge TV-bands database system communications are Internet web services that are built upon and employ open communication standards. Various information services like channel lists and database synchronization utilize web services which are delivered as functions that may be incorporated into an Interface. An Interface is defined as a web service that implements a security model and makes available a defined set of functions.

The Key Bridge white space system provides a number of functional software modules. These include modular component-based implementations of required engineering algorithms and management features for:

- Synchronization between and among multiple databases
- Import, analysis and synchronization of data received from the FCC
- Authenticated and secure Internet communications between the TV bands database and TV band devices
- Assured, positive verification of TV band devices and their FCC certification status
- Geographic information system capabilities that include the accurate calculation of protected services contours
- Management of various user-classes and accounts including FCC staff, protected entities, professional installers and TV band consumers

Application Programmer Interfaces

External system interfaces are two-way, machine-readable web service resources available to authorized devices and persons that provide machine discoverable and readable one or two-way communication resources. The Database administrator or third parties may use external interfaces to build network-based applications that incorporate the Database as an Internet information resource. Examples may include a TV band device channel list query client, etc.

The Key Bridge white space administration system provides two key external interfaces and accompanying APIs that support two-way, machine-to-machine data exchange. These are:

- Channel list query responder web service API for TV band devices
  (via the interface INT-TVBDx)
- Data synchronization service for other Database administrators
  (via the interface INT-SYNC-DB)

Web Portals

Several web services may not be directly accessible to outside parties. Rather, they exist to support Database web portals or other applications. Examples of internal web services are those that support protected services registration, record review and FCC oversight.

There are nine basic Database interfaces defined in the Key Bridge functional architecture. These are described in the following table.

Class	Interface Label	Interface Description
External	INT-TVBD-[X]	A class of functionally similar database web services that provide machine-readable services to TV Band devices. Their primary function is to accept and reply to channel inquiries. Two interfaces are defined for database to device

		communication: • INT-TVBD-F for Fixed class devices • INT-TVBD-2 for Mode-II devices One interface is described but not defined for TVBD Master to Slave communication: • INT-TVBD-1 for Fixed or Mode-II Master to Mode-I slave devices This interface can be extended to accommodate new feature sets or device types.
External	INT-SYNC-DB	An external interface to enable for the synchronization of independently operated TV band database systems
Internal	*INT-RM-TVBD*	*Interface for record management. Allows for the creation of new records for Fixed TV band device records, plus review or modification of existing records*
Internal	*INT-RM-PS*	*Interface for record management. Allows for the creation of new protected service records, plus review or modification of existing records*
Internal	*INT-FCC*	*Interface to accommodate oversight, reporting and enforcement by authorized Commission staff*
Internal	*INT-FCC-CDBS*	*Data collector to retrieve and process CDBS tables, whole or in part, from the FCC*

Internal	*INT-FCC-ULS*	*Data collector to retrieve and process ULS tables, whole or in part, from the FCC*
Internal	*INT-FCC-EA*	*Data collector to retrieve and process Equipment Authorization information from the FCC*

4.6.1 Communications with the FCC

The Key Bridge TV bands Database has four software subsystems that communicate via independent interfaces with the FCC. These are illustrated in Figure 18.

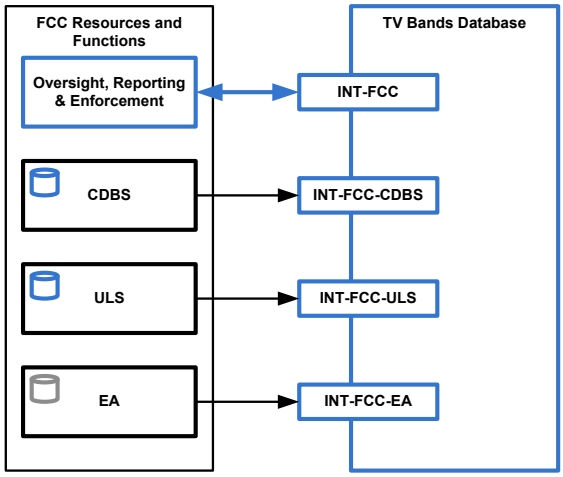


Figure 18: Four independent system interfaces provide secure communications between the TV bands Database and FCC

Two system interfaces (INT-FCC-CDBS and INT-FCC-ULS) provide file retrieval and raw data processing capabilities. One communications interface (INT-FCC-EA) is a custom developed software application that interacts with the FCC's own Equipment Authorization [providing] a machine-readable [Web] service.

Key Bridge anticipates that the Commission will want to monitor initial TV bands deployment and consumer adoption. To enable TVBD audits and enforcement, Key Bridge provides a user-friendly web portal that encapsulates the machine-readable web services interface INT-FCC that supports multiple user roles and responsibility levels.

Through a set of standardized and extensible system interface, Key Bridge reliably gathers, imports and processes raw data from the FCC. It provides comprehensive TV band information reporting capabilities, operational status information and device enforcement functions. Our system modular architecture also allows rapidly incorporating new features as the system, and FCC requirements, evolve with the TV bands marketplace.

4.6.1.1 Collecting Incumbent Records from FCC Data via Daily File Transfer

The Media Bureau provides information from its Broadcast and Cable databases for public download and use. CDBS, or Consolidated Database System, is the relational database used by the Media Bureau to process AM and FM radio plus broadcast television applications.

The FCC Media Bureau dumps a complete version of the CDBS database contents nightly into text files at approximately 4:30 AM Eastern time on the morning after each business day.

The Wireless Bureau provides nightly update files and complete data dumps from its Universal Licensing System (ULS) databases for public download also at approximately 4:30 AM Eastern time on the morning after each business day. Nightly update files only include database changes. ULS data files are available to the public in compressed archive file format (ZIP).

Figure 19 describes the Key Bridge system for collecting information from the FCC. The Commission's two main databases with incumbent transmitter records are CDBS and ULS. As described, CDBS data is available en-bulk via a daily database dump files, whereas ULS data is

exported also en-bulk and with daily transaction files. Equipment Authorization data is not exported, but rather presented via a human readable web portal.

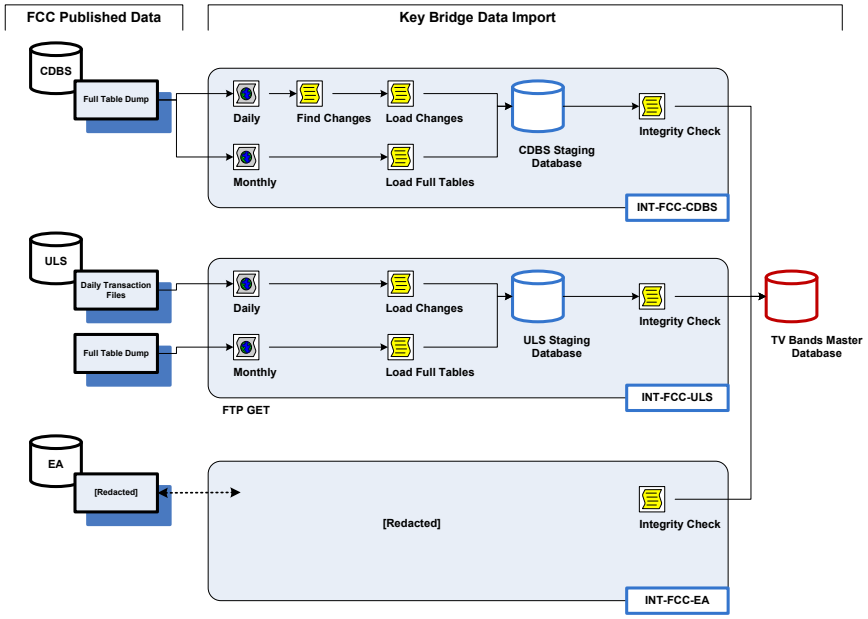


Figure 19: Data and process flow diagram describing how information is collected from sources at the FCC and imported into the TV bands database. CDBS and ULS information is incrementally updated daily and completely refreshed once per week. Equipment authorizations are retrieved on-demand.

Our system retrieves the complete CDBS data files and the ULS transaction files at approximately 6:00 AM Eastern time every day of the week (7 days). Downloaded CDBS data files are compared with the previous day's data to produce a daily transaction file which is imported into a CDBS staging database. Once loaded, the updated CDBS staging database is analyzed to ensure data integrity and is then synchronized with the Key Bridge Master database. ULS daily transaction files are processed similarly.

The Key Bridge CDBS and ULS Staging databases are completely refreshed once per month to assure they, and in turn the TV Bands Master database, do not gradually diverge from the FCC's ULS and CDBS.

When TV band devices query for channel lists they must submit as minimum identifying information their FCC ID and product serial numbers.[3] The Key Bridge solution employs a custom-develop equipment authorization module (see 5.4.1.4: *Equipment Authorization*) to retrieve a device's certification record data on demand. This capability enables us to confirm the validity, certification and authorization status of the inquiring device in near real-time.

4.6.1.2 Identifying and Validating Protected Entity Records

The FCC's CDBS contains approximately 83,000 broadcast television records representing applications in various states of approval processing. Possible record status for broadcast television stations include:

Status	Description
ADD	Proposal to add a channel
APP	Application
APPDID	Application denied by initial Decision in hearing
APPGID	Application granted by initial Decision in hearing
CP	Construction Permit

[3] See §15.713(f), (g)

CP MOD	Modification of a Construction Permit
DEL	Proposal to delete a channel
LIC	License

In its final Opinion and Order the Commission clarified its intent that records in the TV bands database should reflect stations that are serving viewers, and explained that active transmission was only provided by stations with a status of "License" or "Application".[4]

In accordance with Rules and the Commissions intent the Key Bridge TV bands database will provide geographic protection for all records learned via CDBS with status "LIC" and "APP". In cases where the same transmitter may have two records with both "LIC" and "APP" status the record with status "APP" shall have precedence.

The full FCC ULS database contains several million entries across over 80 different tables. ULS data must be filtered to identify the current, active records that must be protected, but there are fewer record status possibilities for entity classes held in ULS. Possible record status options in the ULS database include:

Status	**Description**
A	Active
C	Canceled
E	Expired
L	Pending Legal Status

[4] See FCC 10-174, Second Memorandum Opinion and Order (Order) at paragraph 121.

P	Parent Station Canceled
T	Terminated
X	Unknown

By default, only records with "Active" status are protected by the Key Bridge TV bands database.

4.6.1.3 Converting Geographic Coordinates

Data in the CDBS is stored using the NAD27 DATUM, and is not compatible with either the Commission's other databases, which use NAD83, or modern GPS-based devices, which typically use WGS84. The TV bands database system must therefore contain the capability to convert from NAD27 to NAD83. The system should also contain the capability to convert from WGS84 to NAD83.

4.6.1.3.1 NAD27 to NAD83

Geographic coordinates in the Universal Licensing System reference the North American Datum of 1983 (NAD83), whereas the Consolidated Database System references another, incompatible datum: NAD27.

FCC Rules require the TV bands database to store all geographic information using the NAD83 datum. The TV bands database must therefore translate geographic coordinates from NAD27 to NAD83.

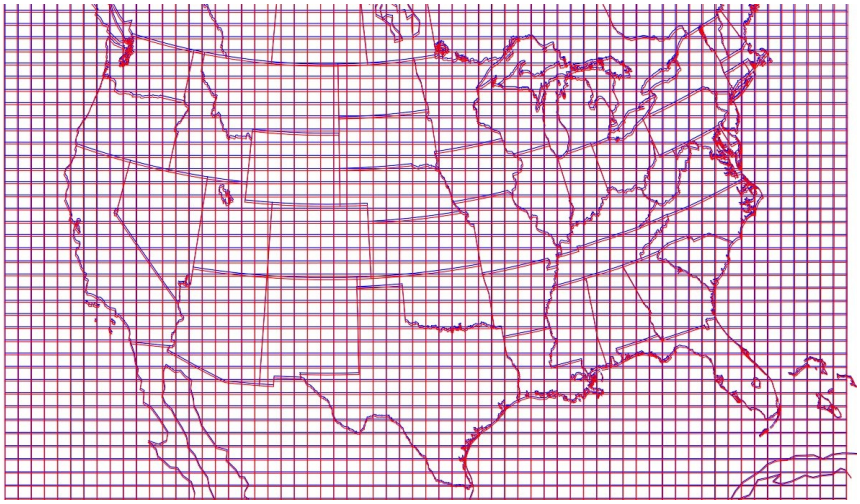


Figure 20: Offset grids showing the variable magnitude of change between NAD27 and NAD83 datum for North America. Blue is NAD27 and Red is NAD83. (Source: NOAA NCEP Grid Number 103)

In 1990, the Federal Geodetic Control Committee adopted the NADCON software package, developed by the National Geological Survey, as the federal standard for conversion to NAD83. The FCC also identifies NADCON software as the preferred method for converting to NAD83 coordinates.

Key Bridge followed FCC public guidance and implemented a NADCON software module compatible with the FCC's coordinate conversion procedures:

For the contiguous 48 states and the District of Columbia), Alaska (including St. Laurence, St. George, and St. Paul Islands), Hawaii, Puerto Rico and the U.S. Virgin Islands, the NADCON software module employs Version 2.1 of the NADCON software with the following parameters:

	Latitude (degrees)		**Longitude (degrees)**	
Location	**min latitude**	**max latitude**	**min longitude**	**max longitude**

CONUS	20	50	63	131
Hawaii	18	23	154	161
Puerto Rico and USVI	17	19	64	68
AK - St. Laurence Island	62	64	168	172
AK - St. George Island	56	57	169	171
AK - St. Paul Island	57	58	169	171
Alaska	46	77	128	194

For the unincorporated territory of American Samoa, the following datum shifts are used:

- For Tutuila Island:

  lat, long (NAD83) = lat (NAD27) - 17.83406", long (NAD27) + 4.37866"

- For the Manua Islands:

  lat, long (NAD83) = lat (NAD27) - 18.32515", long (NAD27) + 4.43134"

For the unincorporated territory of Guam, the following datum shift is used:

- For Guam:

  lat, long (NAD83) = lat (NAD27) + 5.15932", long (NAD27) + 8.71596"

4.6.1.3.2 WGS84 to NAD83

As background, the US Department of Defense (DoD) established the original WGS84 reference frame in 1987 using Doppler observations, and in 1994, DoD introduced a version of WGS 84 exclusively based on GPS observations. While WGS84 tracks the Earth center of mass, NAD83 tracks the movement of the North American plate. The WGS84 and NAD83 datum were identical in 1987 and have since diverged approximately between 3 and 4 feet.

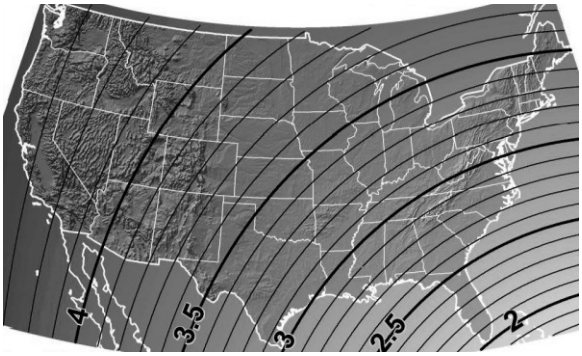


Figure 21: 2002 horizontal differences between NAD83 and WGS84 datum, in feet

Most GPS devices, likely to include TVBDs, may reference the NAD83 datum but are typically configured to reference the WGS84 datum by default.

The Key Bridge solution supports coordinate transformations from WGS84 coordinates to NAD83. The relative shift between the WGS84 datum and NAD83 datum is modeled by a 14-parameter transformation matrix dependent upon a position's latitude, longitude, altitude and date, reflecting the following values:

Parameter	**1997**		**Velocity**		**2009**	
Value	**Reference**		**per Year**		**Value**	
DX	0.9956	m	0.0007	m	1.004	m
DY	-1.9013	m	-0.0007	m	-1.91	m
DZ	-0.5215	m	0.0005	m	-0.515	m
RX	0.025915	"	0.000067	"	0.02672	"
RY	0.009426	"	-0.000757	"	0.00034	"
RZ	0.011599	"	-0.000051	"	0.01099	"

Scale	0.00062	ppm	-0.00018	ppm	-0.0015	ppm

4.6.1.4 Equipment Authorization

The TV bands database must confirm all inquiring TV band devices are FCC certified for unlicensed operation in the television broadcast bands.

Most electronic devices, including TV band devices, are required to meet certain FCC technical requirements before they can legally be imported or sold in the USA. Devices are assigned, and may display, an FCC ID number when it has received an FCC grant of Equipment Authorization.[5]

The FCC ID consists of two elements:

- A grantee code
- An equipment product code

The Grantee code is a three character alphanumeric string unique to each Grantee/Applicant. The Grantee Code always begins with an alphabetic character and does not contain the numbers one and/or zero. The Commission assigns a Grantee Code permanently to companies for authorization of their radio frequency equipment.

The Product Code is the rest of the FCC ID that begins after the first three characters. The Product Code may include hyphens and/or dashes (-).

FCC's Office of Engineering and Technology (OET) is responsible for the authorization of radio devices, and provides an electronic search capability to the Equipment Authorization System

[5] Under various Title 47 rules including but not limited to Parts 15, 90, and 101

(EAS) database. The Key Bridge TV bands database system retrieves device certification status by directly interfacing with the FCC's Equipment Authorization System.

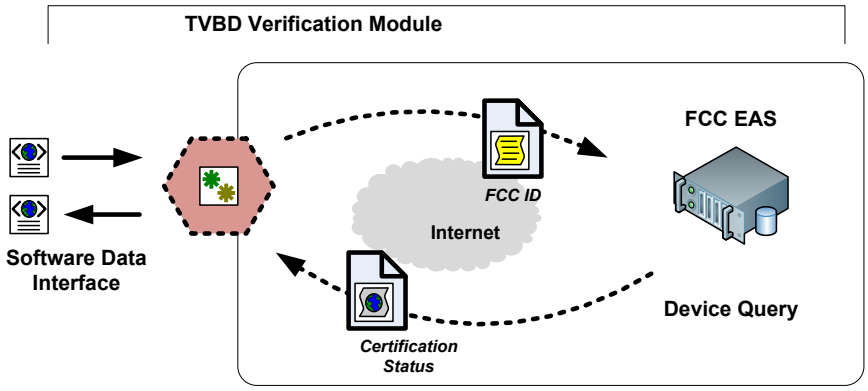


Figure 22: The Key Bridge TVBD Verification system provides an automated, machine-readable method to confirm device certification status. The software provides a standards-compliant Equipment Authorization Web service.

The Key Bridge TVBD verification system provides an automated, machine-readable resource with the following functions:

- Confirm in near real-time and based upon FCC ID that an inquiring device is FCC certified
- Validate that the device is certified to transmit in TV bands frequencies
- Identify specific TV channels that the device is certified to operate on

  (We do not assume 100% frequency coverage)

The Key Bridge EA solution is shown in Figure 22, while the module's collection and processing method is illustrated in Figure 19.

4.6.1.5 Oversight, Reporting and Enforcement

As described in §15.713(i), the Commission may wish to request and receive standard TV bands white space reports and information. Additionally, as with any new technology deployment, the

Commission may be required to make certain enforcement actions from time to time. Key Bridge provides a flexible oversight, reporting and enforcement capability built upon a flexible web services architecture that may provide comprehensive and convenient access to the Commission.

Referring to Figure 23, certain tables may be exported from the Key Bridge TV bands Master Database (shown in red) and synchronized to a dedicated Slave database instance (shown in blue) which may be dedicated for supporting Commission access. Data for Commission consumption may then be securely exported via a subtended slave instance (shown in black) and a set of dedicated web services (also illustrated).

A secure web portal with integrated mapping capability will provide the Commission with a convenient user interface to the system through which the Commission may execute any number of desired report queries. Using the web portal Commission staff may also review Database contents and test various aspects the Database's functionality at their convenience.

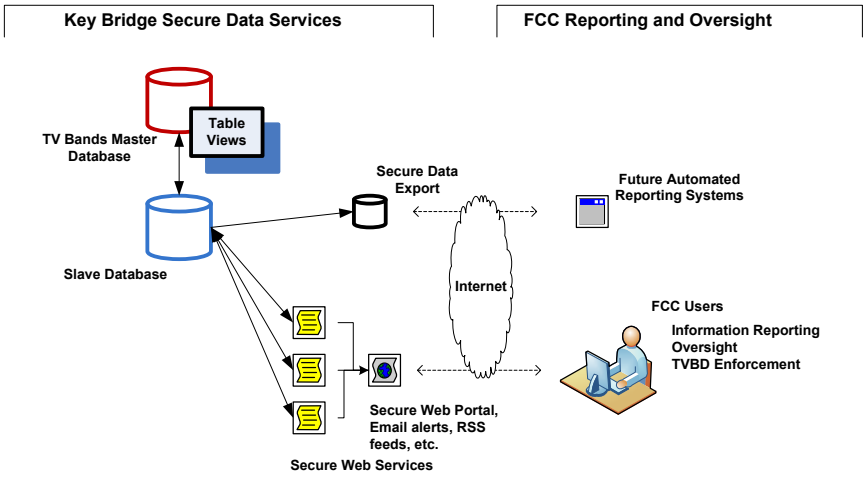


Figure 23: Resources available to the Commission for ad-hoc information query, report generation and TVBD enforcement. Secure database exports (black) accommodate additional automation and/or third party systems integration in the future.

The web portal may provide several preconfigured functions the Commission may employ for status reporting and enforcement where necessary. Examples may include:

- A channel status inquiry may report all active TV band devices on an indicated channel within a desired geographic area of interest.
- A device status inquiry may produce an operational history report of a class of TVBD and a specific device if one is indicated. Operational history may include the locations and times of device channel list inquiries.

All TVBD must support a Commission enforcement requirement to disconnect a specific device, class of devices, or all devices on a specific channel. Through a dedicated Web portal the Commission may preclude:

- A specific device from receiving channel lists
- An entire class of TV band devices from receiving channel lists

Positive enforcement requires a message exchange originated by the Database to active Fixed and Mode-II devices. While not required by the Commission's rules, the Key Bridge TV bands system may support this capability.

4.6.1.5.1 FCC Black List

A list of devices the Commission may preclude from receiving a channel list may be describes as a 'Black List', which is a list or register of entities that are denied a particular privilege, service, mobility, access or recognition. Conversely, a "White List" may be defined as a list or register of entities that are accepted, recognized, or privileged.

The Key Bridge TV bands system does not incorporate a white list. Rather, all duly certified TV band devices are allowed by default. Only a Commission provided black list of devices that may not receive channel lists will be maintained by Key Bridge.

The Commission may update a registry of disallowed devices (e.g. a black list) at any time. In the Key Bridge system, any changes to the black list that the Commission may provide are immediately exported for synchronization with other designated White Space administrators.

4.6.2 Protected Entity Registration

The Database must enable the registration of certain protected entities not already in the FCC's CDBS and ULS databases. This is required to provide interference protection from unlicensed devices to authorized spectrum users or transmission infrastructure. Facilities and services not recorded in the Commission databases but entitled to interference protection include:

- Multi-channel Video Programming Distributor (MVPD) receive sites[6]
- Translator, Low power and Class A television station receive sites[7]
- Low power auxiliary stations, including wireless microphones and wireless assist video devices[8]

These enumerated entities are entitled to receive protection from interference from unlicensed TVBDs and may therefore voluntarily register their facilities and events with the TV bands database. The Key Bridge Database solution accommodates both individual (single site) and

[6] See §15.713(h)(6)

[7] See §15.713(h)(7)

[8] See §15.713(h)(8), (9)

automated (multi-site) registration of voluntary protected entities through a set of web services and web portals. Protected services registration and records management are bundled in the system interface labeled 'INT-RM-PS'.

4.6.2.1 Registering MVPD Receive Sites

Key Bridge provides for convenient registration and management of cable head end protections via a web portal. Authorized company representatives may register for protection. Key Bridge provides three methods for establishing and managing MVPD receive site records:

- Web service
- Web portal
- Manual processing

MVPD receive sites may be registered en-bulk via a dedicated web service, for which Key Bridge may provide a standard software API and security framework and that companies integrate directly into their own back-office systems.

MVPD receive site facilities and channels may also be registered and managed via a Key Bridge-provided web portal. The cable web portal encapsulates the MVPD web service described above and allows for creation, review and management of all MVPD receive site information.

Lastly, Key Bridge will accept MVPD receive site information via electronic format submitted directly by an authorized company representative. Key Bridge provides a spreadsheet template that company representatives may use submit location and channel use information to Key Bridge technicians for import into the database system.

4.6.2.2 Registering Translator, Low power and Class A Television Station Receive Sites

Key Bridge for convenient registration and management of television receive sites via the Database interface 'INT-RM-PS'. The TV bands database learns 'Licensed' or "Application" television records from FCC provided information in the CDBS database. From CDBS each record may be associated to a company and responsible individual. Similar to the procedures created for MVPDs, Key Bridge may provides for the registration of television receive sites via three methods:

- Web service
- Web portal
- Manual processing

Key Bridge may provide a standard software API and security framework for authorized third parties to integrate directly into their own back-office systems. Television receive sites and channels may also be individually registered and managed via a Key Bridge-provided web portal. The web portal encapsulates the web services described above and allows for creation, review and management of all necessary information.

Lastly, Key Bridge will accept television receive site data in electronic format submitted directly by authorized individuals. Key Bridge provides a spreadsheet template television representatives may use to submit receive site and channel information to Key Bridge technicians for import into the database system.

4.6.2.3 Registering Low Port Auxiliary Stations (Licensed)

Low power auxiliary stations, including wireless microphones and wireless assist video devices (collectively LPAUX), may be entitled to one or more circular protected contours, each with a

fixed radius of 1 km for Fixed TVBDs and 400 meters for personal/portable TVBDs.[9] Where more than one contour is created the contours must touch or overlap to be considered part of the same registration. As illustrated in Figure 24 the net protected contour is the union of each individual protected contour and may be represented as a continuous, larger contour with no holes.

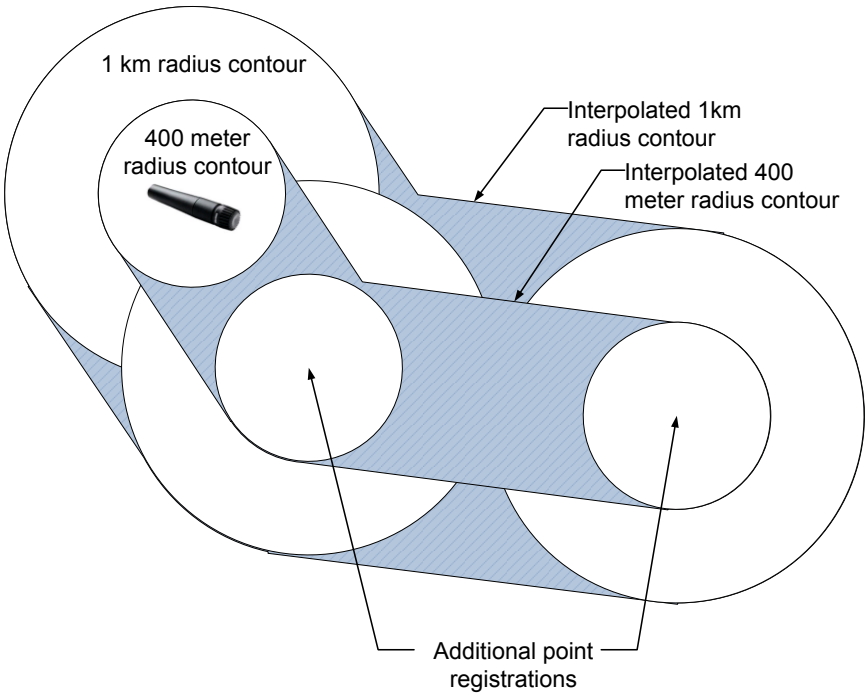


Figure 24: Example LPAUX reservation illustrating multiple 1km/400 meter registrations and how multiple registrations may be joined together to create a contiguous enclosed area which is automatically filled. The net protected contour is the outer border from a union of all 1 km/400 meter circles.

[9] See §15.712(f)(1) and §15.713(h)(8), (9)

Key Bridge provides convenient methods for convenient registration and records management of licensed and unlicensed LPAUX stations via the Database interface 'INT-RM-PS'. The Key Bridge TV bands database accepts single and multiple enrollments via a web portal.

The Key Bridge LPAUX system is designed similar to other event registration systems that incorporate a persistent user profile. Once enrolled, individuals and company representatives may associate locations, equipment, frequencies and schedule of events to their account. Users may identify one or more protected services contours for activation by associating their location, frequency and event schedules with a responsible party (contact person).

In its simplest form, all information is submitted to the Database and managed by a single individual. The Key Bridge web portal solution is convenient and easily accommodates small or fixed installations like churches, high schools and theaters.

The Key Bridge solution also allows companies to create separate functional roles with varying degrees of authority. For example, event data (location, frequency, schedule, contact person) may be created by one group of users while event activation is reserved for another. The Key Bridge microphone registration solution allows separation of responsibilities and authorities among groups to accommodate large, complicated LPAUX use cases like major sporting events and travelling concerts.

Key Bridge exposes the TV band database LP-AUX reservation system through a set of web services and a convenient web portal for end users:

- Web service
- Web portal

Key Bridge provides a standard software API and security framework that third parties may use to integrate and automate LP-AUX registration and management directly into their own back-

office or end-user systems. The LP-AUX web portal encapsulates the web service described above and allows for creation, review and management of all necessary record data via a Web browser.

Key Bridge will accept LPAUX data in electronic format submitted directly by authorized individuals on a case-by-case basis. Key Bridge provides a spreadsheet template television that individuals or companies properly format information for Key Bridge technicians for import into the database system.

4.6.2.4 Registering Low Port Auxiliary Stations (Unlicensed)

§15.719(h)(9) anticipates a process whereby "the Commission will provide [unlicensed microphone registration] information to the Database managers." Key Bridge will accept and accommodate whatever structure, format and process for collecting and distributing unlicensed LPAUX registration information the Commission may establish.

4.6.3 Incumbent Record Verification, Correction and Removal

FCC rules require the Database to support record verification, correction and removal by the FCC or other (presumably authorized) party.[10] Key Bridge provides a comprehensive set of resources that enable records review collectively exposed through the 'INT-RM-PS' database interface. These resources are available in two formats:

- Web service
- Web portal

[10] See §15.715(i)

Key Bridge provides standards-compliant web services, software API and a security framework that third parties may use to develop their own automated records inquiry, verification and automation applications. A custom web portal also provides a convenient geographic query and visualization capability of transmitter records in the Key Bridge TV bands database. A mapping capability is incorporated, and protected service contours are available to authorized users via a web browser.

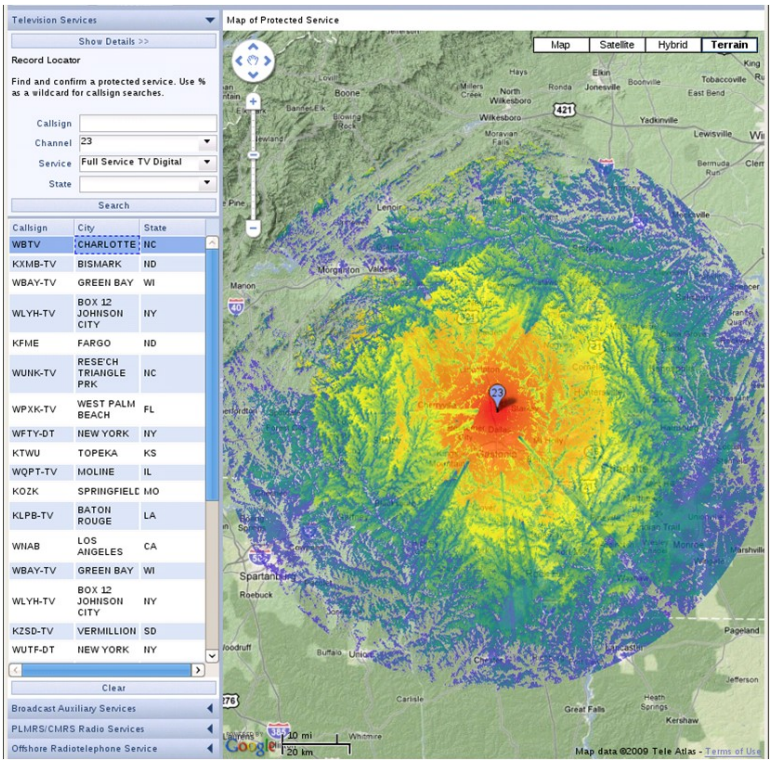


Figure 25: Screenshot of Key Bridge's web portal for incumbent record verification, correction and removal. Shown is the television station browsing interface with area propagation analysis enabled.

The web service and web portal provide similar capabilities. Depending upon their degree of authorized access, individuals may search, review and verify the content of records learned from the FCC via CDBS and ULS and directly registered records like cable head-ends and LP-AUX

events. Users may not edit data that the TV bands database receives from the FCC via CDBS or ULS, but rather may manually flag a record as requiring attention, and Key Bridge may support records correction within the FCC's own CDBS or ULS databases.

4.6.4 TV Band Device Registration

FCC rules require the Database to support registration of fixed television band installations.[11] Security requirements and practical necessity may also require that commercial accounts are maintained for TVBDs. In the Key Bridge system, device registration, a prerequisite for receiving channel list services, is not coupled in any way with the creation of a commercial account. Device registration and commercial accounts are neither prerequisites nor requirements of one another and may be established and maintained separately by independent parties.

Key Bridge provides a flexible set of procedures and resources for manufacturers, service providers and end-users to conveniently and securely registration and maintain device registration information via the Database interface 'INT-RM-TVBD'.

The TV bands database accepts enrollment of individuals and businesses, via the Internet, to create accounts that may register Fixed or Mode-II TVBDs. Presently there are no restrictions on enrollment. The Key Bridge TVBD system is similar to other registration platforms that incorporate a persistent user profile. Once enrolled, individuals or company representatives may associate, individually or en-bulk, equipment, locations and contact persons for fixed TVBD installations. While the records and association process for Mode-II TVBDs is similar to that for Fixed devices, only commercially necessary information is required and the rest is made optional.

[11] See §15.715(c)

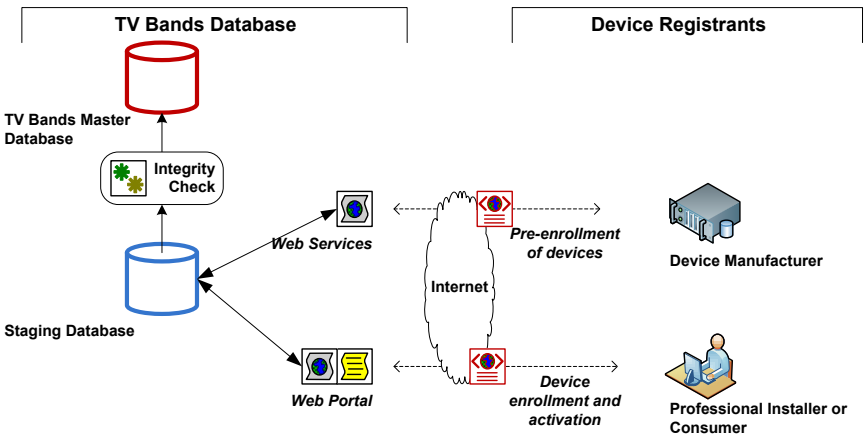


Figure 26: Schematic showing pre-enrollment by device manufacturers and enrollment plus activation by a professional installer. Personal/portable users (e.g. consumers) may also register devices to receive channel lists via a consumer version of the professional installer's web portal. Only encrypted data is exchanged across the Internet (Red).

Key Bridge very much wishes to minimize any burden on consumers and barriers to successful, widespread commercial adoption, and day-to-day operation of Fixed and Mode-II TVBDs may require a direct commercial account between the TVBD user and Key Bridge. This is particularly important for Mode-II consumer products intended to be sold at retail, like home gateway routers and wireless access points. The Database may charge for channel lists to cover the cost of operation.[12] The Key Bridge solution therefore accommodates both manual and automated registration and maintenance of TVBD information through a set of web services and web portals.

[12] See §15.714 (a)

For clarity, registration is creation of an active, valid and complete record in the Database. Registration is a prerequisite for unlicensed operation of Fixed or Mode-II TV band devices and for the protection of services not in the FCC's databases.[13, 14]

The full complement of secure TVBD registration web services on 'INT-RM-TVBD' are available to device manufacturers, network service providers and retail sales channels to enable automation and integration into their back office systems, while a TVBD registration web portal encapsulates the web service described above and allows for creation, review and management of devices and records by professional installers and consumers.

4.6.5 Flexible Options for Database Synchronization

Key Bridge implements a publish/subscribe strategy for database synchronization between and among multiple TV bands administrators.

Publish/subscribe (or pub/sub) is an asynchronous messaging paradigm where senders (publishers) of messages are not programmed to send their messages to specific receivers (subscribers). Rather, published messages are characterized into classes, without knowledge of what (if any) subscribers there may be. Subscribers express interest in one or more classes, and only receive messages that are of interest, without knowledge of what (if any) publishers there

---

[13] See §15.713 (b)(2)

[14] Fixed device Registration may require both a record of the device's identifying information as defined in 47 CFR §15.713 (f)(3) in the Database and a commercial account with the Database administrator. Mode-II TVBDs are not required to maintain a record in Database but may require a commercial account with the Database administrator for the settlement of fees.

are. This decoupling of publishers and subscribers can allow for greater scalability and a more dynamic network topology.

The Key Bridge synchronization model employs a one-way synchronization whereby the subscriber's state (Party B) is updated to match the Publisher (Party A). For complete synchronization to occur, a parallel process must also run in the opposite direction, with roles reversed. As a practical matter, parties must ensure they do not re-publish, or round-trip, the data they receive. During normal operation, the Publisher may continually make available (publishes) information updates in a convenient, standards-based machine-readable format. Subscribers bear the responsibility to successfully retrieve and process and import the data.

Key Bridge publishes various types of data requiring different synchronization schedules using the following methods. These are:

- Database-to-database peering
- Asynchronous Messaging
- Bulk file transfer

Key Bridge database synchronization employs a multi-stage system to ensure data integrity, availability and compatibility for subscribers, illustrate in **Error! Reference source not found.**, where a dedicated, slave database instance (shown in blue) is configured to receive real-time updates of the required synchronization data from the TV bands master database (shown in red).

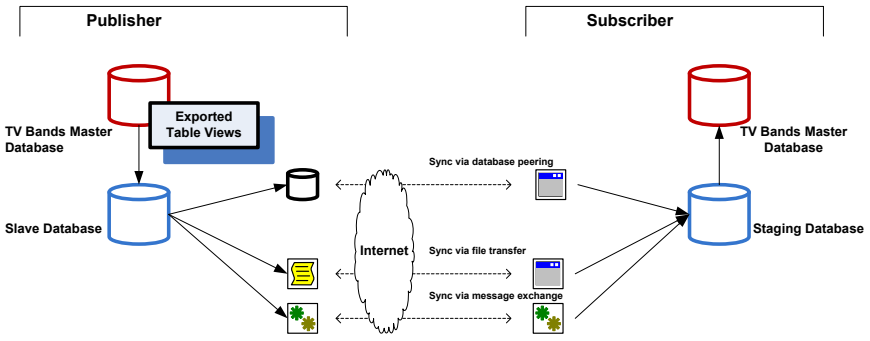


Figure 27: Key Bridge database synchronization service publishes data in several formats, allowing subscribers to retrieve updates in near real-time via database-to-database peering, near real-time via asynchronous messaging, or periodically via bulk file transfer.

For synchronization via database-to-database peering the slave database is configured to serve as a master database for replication into an exported database instance (shown in black), which may be made available to other administrators. Database peering provides near real-time synchronization.

Other administrators not able to synchronize Key Bridge via direct database peering but wishing to enable near real-time synchronization for time-sensitive records exchange may subscribe to a Key Bridge provided GlassFish Message Asynchronous Queue instance. Messages containing database transaction updated are published in near real-time to the Queue and may be retrieved at the subscriber's convenience. Example transactions published to the Queue may include, e.g., for example ad-hoc licensed microphone registrations supporting electronic news gathering operation.

In a similar fashion as the Commission's strategy for CDBS and ULS, Key Bridge provides a nightly dump of the entire content of exported data in a raw text file that may be available for secure retrieval by authorized administrators.

By these methods, other Database administrators may ensure they are properly synchronized with the Key Bridge system.

4.6.5.1 Near Real-Time Synchronization by Database-to-Database Peering

Key Bridge prefers to synchronize with other administrators via database-to-database peering. Key Bridge will publish synchronization information using the MySQL database.

MySQL supports asynchronous replication between singleton or cluster installations in any number of master/slave configurations. Replication mirrors data in near real time between

geographically distant databases installations across a WAN. Database replication is between a master and a slave server. The master server is the initiator of the operation while the slave listens and receives incoming instructions and data. A MySQL server can be configured to operate as a Master or Slave at different times. In some cases may be a Master and Slave at the same time.

During replication, updates to a master database (i.e. record adds, drops & changes) are recorded and transmitted to a slave system. A dedicated software process on the Master server creates indexed and time stamped binary log entries that are immediately forwarded to the slave database.

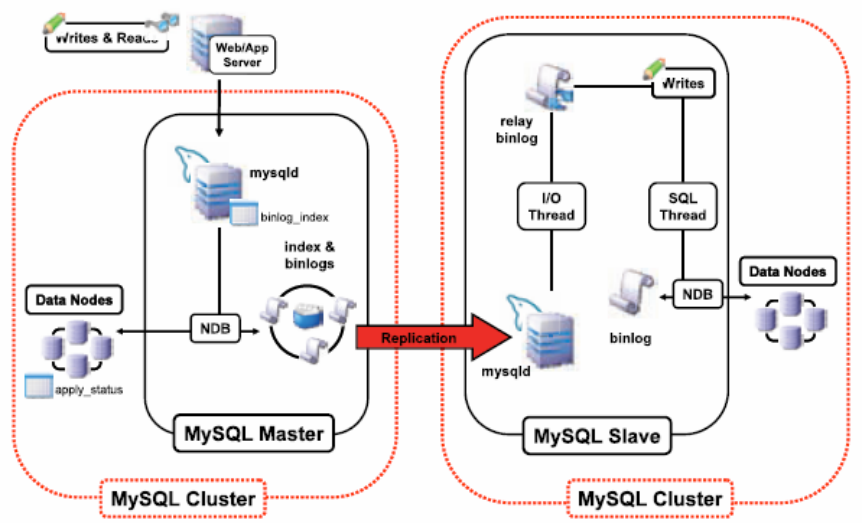
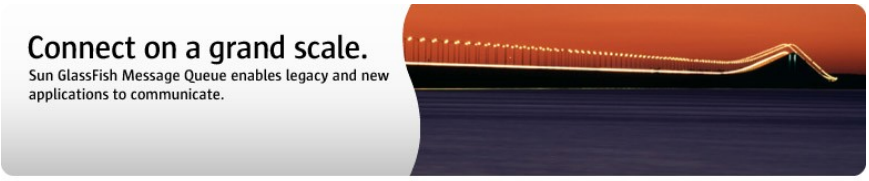


Figure 28: Example showing a single MySQL master server replicating to a slave instance. The Master server creates and forward binary log messages to the Slave system.

4.6.5.2 Near Real-Time Synchronization by Message Queue



In computer science, message queues are software-engineering components that provide an asynchronous communications protocol for the exchange of data. Messages placed onto the queue are stored until the recipient retrieves them. Message queues allow for reliable exchange of encapsulated data between computer systems, potentially connecting multiple applications and multiple operating systems.

The Key Bridge TV bands database solution employs Sun's Glassfish Message Queue system to publish database update messages via an open standard protocol called Java Message Service (JMS), which is widely supported and open source. The Key Bridge Synchronization Message Queue provides a number of important services:

- Provides scalability, reliability, and advanced security necessary for large-scale deployments
- Ensures support for once-and-only-once message delivery
- Ensures only authorized individuals receive messages, which are tamper-proof and confidential
- Includes clustering and load distribution for high availability and high performance
- Supports near real-time database updates

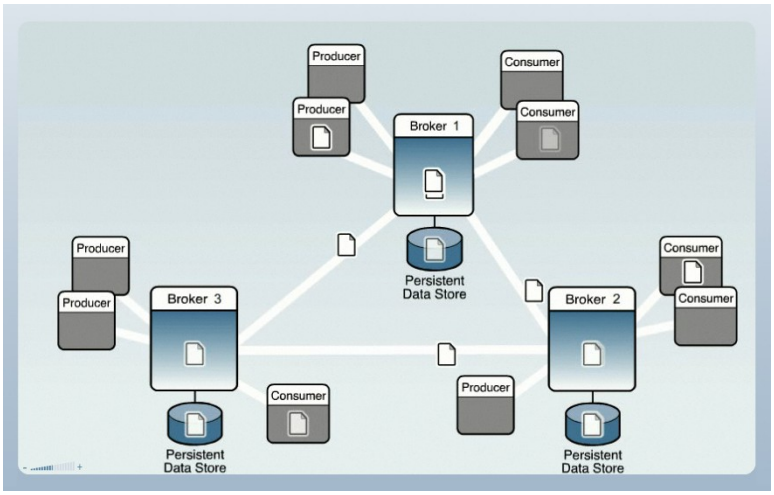


Figure 29: Example of a three-node high-availability system providing high-availability asynchronous messaging. Message producers and consumers may connect to the network at any time, with secure, assured delivery.

4.6.6 Calculating Protected Services Contours

The Database must calculate, on demand and for any given geographic location, the radial distance between an inquiring TV band device and the protected service contour of all nearby protected entities. This requires two important system functions:

- calculating the protected service contour, and
- calculating the geographic distance between the protected transmitter and the inquiring TVBD.

If the contour distance is less than the device's separation distance the protected transmitter's channel may be available for unlicensed operation by the TVBD.

There are several classes of protected entity, each with a uniquely defined geometry describing their geographic protected contour. These are listed in Figure 30.

In the Key Bridge TV bands database system, a dedicated software module handles each class of service contour calculation. Algorithms in each respective software module implement the required protection algorithms, methods and practices.[15]

Service Type	Typical Protected Contour* (* radius + geometry)
Broadcast TV 	F(50,50) or F(50,90) defined
TV Translators & Cable Head Ends 	80 km Slice + 8 km Circle
Broadcast Auxiliary 	80 km Slice + 8 km Circle
PLMRS / CMRS 	134 km Circle + 50 km circle
Wireless Microphones 	1 km Circle(s) or User-defined
Border Areas 	32, 40 or 60 km from Border
Offshore Radiotelephone 	Defined area
Radio Astronomy 	2.4 km Circle

Figure 30: Eight classes of protected entity are defined in the Rules, each with a uniquely describe geographic contour.

4.6.6.1 Calculating Geographic Distance [16]

Several software modules developed and commonly used in the Key Bridge system provide standard geographic calculations of distance and course angle between two geographic points. These methods are derived 47 CFR §73.208. They provide basic calculating functions wherever

[15] See Key Bridge: *Interference Protection Requirements* for a detailed examination of the rules, interpretation and protection algorithms.

[16] From 47 CFR §73.208

geographic distances and angle calculations are required to determine protected contour geometries.

47 CFR § 73.208 Reference points and distance computations.

(c) The method given in this paragraph shall be used to compute the distance between two reference points, except that, for computation of distance involving stations in Canada and Mexico, the method for distance computation specified in the applicable international agreement shall be used instead. The method set forth in this paragraph is valid only for distances not exceeding 475 km (295 miles).

(1) Convert the latitudes and longitudes of each reference point from degree-minute-second format to degree-decimal format by dividing minutes by 60 and seconds by 3600, then adding the results to degrees.

(2) Calculate the middle latitude between the two reference points by averaging the two latitudes as follows:

$$ML = (LAT1_{dd}+LAT2_{dd}) \div 2$$

(3) Calculate the number of kilometers per degree latitude difference for the middle latitude calculated in paragraph (c)(2) as follows:

$$KPD_{lat} = 111.13209 - 0.56605 \cos(2ML) + 0.00120 \cos(4ML)$$

(4) Calculate the number of kilometers per degree longitude difference for the middle latitude calculated in paragraph (c)(2) as follows:

$$KPD_{lon} = 111.41513 \cos(ML) - 0.09455 \cos(3ML) + 0.00012 \cos(5ML)$$

(5) Calculate the North-South distance in kilometers as follows:

$$NS = KPD_{lat}(LAT1_{dd} - LAT2_{dd})$$

(6) Calculate the East-West distance in kilometers as follows:

$$EW = KPD_{lon}(LON1_{dd} - LON2_{dd})$$

(7) Calculate the distance between the two reference points by taking the square root of the sum of the squares of the East-West and North-South distances as follows:

$$DIST = \sqrt{NS^2 + EW^2}$$

(8) Round the distance to the nearest kilometer.

(9) Terms used in this section are defined as follows:

(i) $LAT1_{dd}$ and $LON1_{dd}$ = the coordinates of the first reference point in degree-decimal format

(ii) $LAT2_{dd}$ and $LON2_{dd}$ = the coordinates of the second reference point in degree-decimal format

(iii) ML = the middle latitude in degree-decimal format

(iv) KPD_{lat} = the number of kilometers per degree of latitude at a given middle latitude

(v) KPD_{lon} = the number of kilometers per degree of longitude at a given middle latitude

(vi) NS = the North-South distance in kilometers

(vii) EW = the East-West distance in kilometers

(viii) DIST = the distance between the two reference points, in kilometers

4.6.6.2 Calculating the Course Angle between Two Points [17]

It directly follows from 47 CFR §73.208, cited above, that the initial course angle, theta, measured from point 1 to point 2 can be obtained by a simple trigonometric transformation. As in 47 CFR §73.208 , this is assumed accurate only for relatively short distances (< 475 km) where the Earth's curvature introduces only a marginal effect on internal spherical angles. The course angle between two points P1(lat_1, lat_2) and P2(lat_1, lat_2) may be calculated as:

$$\theta = \text{atan}\left(\frac{\text{lon}_2 - \text{lon}_1}{\text{lat}_2 - \text{lat}_1}\right)$$

For distances greater than 475 km spherical coordinates and the following set of equations may instead be used. For two points not on either pole, where the vector has negative slope, the course angle between those two points is described by:

$$\theta = acos\left(\frac{\sin(lat_2) - \sin(lat_1) * \cos d}{\sin d * \cos(lat_1)}\right)$$

For two points not on either pole, where the vector has positive slope, an simple adjustment is required:

$$\theta = 2\pi - \text{acos}\left(\frac{\sin(lat_2) - \sin(lat_1) * \cos d}{\sin d * \cos(lat_1)}\right)$$

where *d* is the distance between the two points.

The vector slope is defined as:

$$\varphi = \sin(lon_2 - lon_1)$$

[17] Derived from 47 CFR §73.208

4.6.6.3 Calculating Broadcast Television Contours [18]

The TV bands database calculates service protected contours using the F(50,50) and F(50,90) curves. The method is as follows:

1. Calculate the transmitter's **radial HAAT** value in the direction of the TV band device
2. For the radial pointing to the TV band device:
    a. Calculate a corrected **radial ERP** value by multiplying the television broadcast facility's rated ERP with the broadcast antenna's directional loss
    b. Calculate a radial **contour distance** using the appropriate F(50,50) or F(50,90) curve algorithm using, as inputs, the radial HAAT value (Step 1) and the radial corrected ERP value (Step 2a), following the method described in the Federal register.

The method of calculating protected services contours for broadcast television stations is detailed in CFR §73.684 and other Key Bridge documents and illustrated in Figure 31.

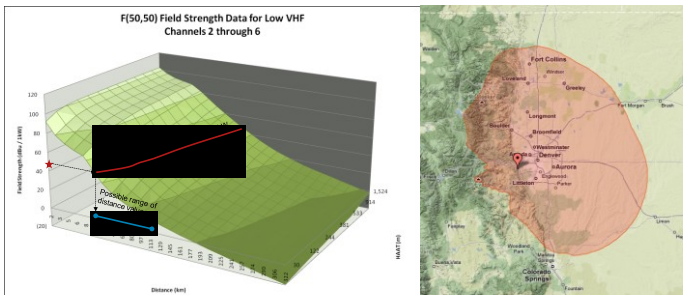


Figure 31: Left: Plot of F(50,50) curve for Channels 2-6 as a 3D surface illustrating the method to solve for Distance using specified field strength and HAAT values. On the right

[18] See §73.684

is an example plot of the TV service protected contour for KRMA-TV channel 18 in Denver, CO, iterating the illustrated method and incorporating radial HAAT values.

As a historical note, the Commission's F(50,10) and F(50,50) curves represent normalized empirical measurements of the variances in field strength power as the transmitting antenna height above average terrain (HAAT) and distance from the transmitter are varied. Radio propagation is frequency dependent, and the Commission provides three sets of curve data to accommodate VHF Low (Channels 2-6), VHF High (7-13) and UHF frequencies (14-69). The Commission's F(50,90) curves represent a calculated extrapolation from the F(50,10) and F(50,50) empirical data sets.

4.6.6.3.1 Calculating Radial HAAT

Height above average terrain (HAAT) is used extensively in FM radio and television and is an important factor in determining the range of broadcasts. HAAT is important for line of sight VHF and UHF transmissions in particular.

Key Bridge combines a transmitter's height above mean sea level and location with a geographic digital elevation model to calculate that transmitter's radial HAAT for any given direction at any location on the globe.

The height above average terrain (HAAT) for a station is determined from topographic maps by averaging the elevation above mean sea level (AMSL) at points along several radials or radii. This value is subtracted from the elevation AMSL of the antenna, including both the tower itself and the ground it is on, to determine the difference. Negative numbers for HAAT sometimes result from this when the station or airport is in a valley, which is significantly lower AMSL than

the surrounding mountains. In the rare case that a location is below sea level, AMSL itself is a negative number.

An example of two Radial HAAT calculations is plotted in Figure 1 illustrating the effects of mountainous versus relatively flat terrain.

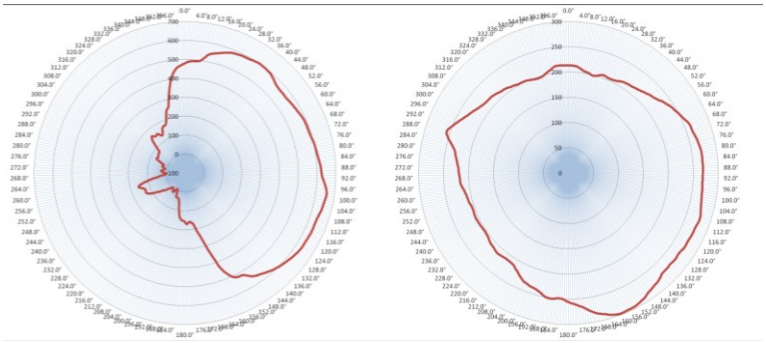


Figure 32: Plot of two Radial HAAT calculations. The attenuating effect of mountainous terrain is visible in the leftmost plot.

4.6.6.4 Calculating Translator, Low Power and MVPD Receive Site and Fixed BAS Link Contours

Translator, Low Power and MVPD receive sites are always paired with a television transmitter. The two geographic points of transmitter and receiver fully define the protected service contour. The TV bands Rules describe similar protected contour geometries for television translator and MVPD receive sites; namely a “key hole” shaped contour originating from the protected receiver with a fixed circular contour and extended arc with dimensions determined by the relative locations of the transmitter and receiver. Both are illustrated in Figure 33.

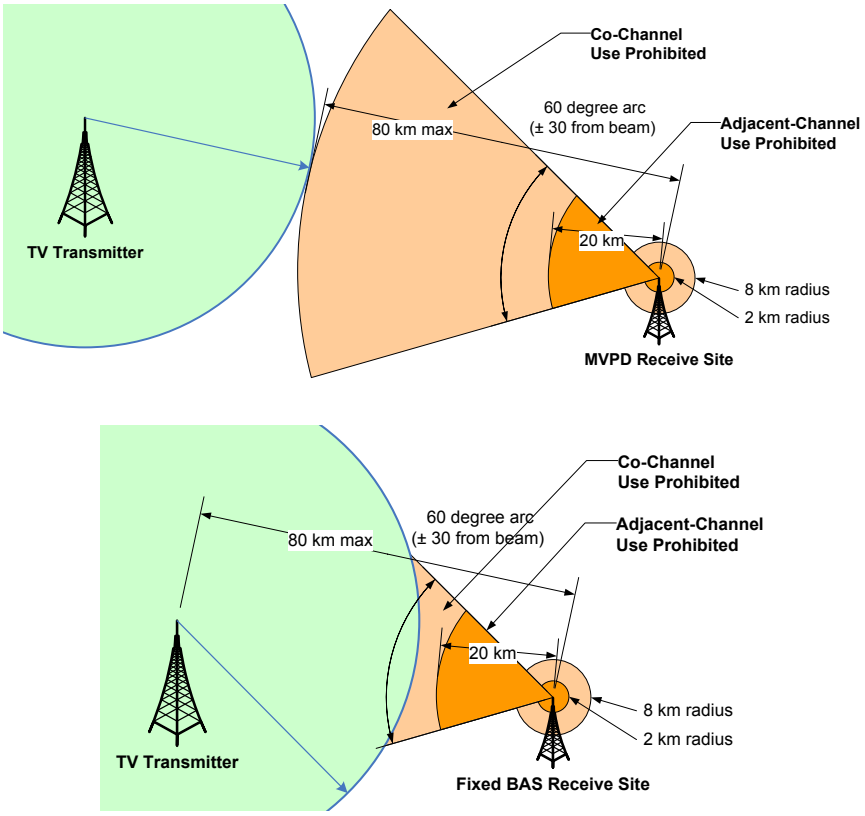


Figure 33: Illustration of Cable Head End protected contours on the left with TV transmitter and fixed broadcast auxiliary service protected contours on the left.

The maximum allowed distance between a television protected contour's edge to the translator or MVPD receiver site (RX) is 80 km, while allows for an extended distance between the receiver and transmitter, while the distance between a protected BAS receiver and television transmitter is limited to 80 km.

To calculate a translator/MVPD/BAS link protected contour the Key Bridge Database first calculates the distance between transmitter and receiver to ensure the receive site is within the 80 km (or 80 km plus contour radius) limit and entitle to protection. The Database then calculates

the inverse course angle (pointing from RX site to TX site) and determines channel protection as follows:

- If the inquiring TVBD is within either of the transmitter's 8 or 2 km inner contours the channels are NOT available
- If the inquiring TVBD lies within an 80km co-channel or 20km adjacent channel radius to the RX site, and is within the +/- 30 degree arc, the protected channels are NOT available

4.6.6.5 Calculating PLMRS / CMRS Contours

The Rules describe a simple circular radius around 13 enumerated metropolitan centers with accommodations for an additional circle extending the protected contour for co-channel and adjacent channel protection.[19] Protected contours are represented as circles with fixed radii of 134 and 131 km for co-channel and adjacent channel frequencies, respectively. Base station contours are circles with fixed radii of 54 an 51 km for co-channel and adjacent channel frequencies, respectively. This is illustrated in Figure 34, where PLMRS/CMRS protected contours are shown as the union of both described geometries, where applicable.

[19] See §75.712(d)

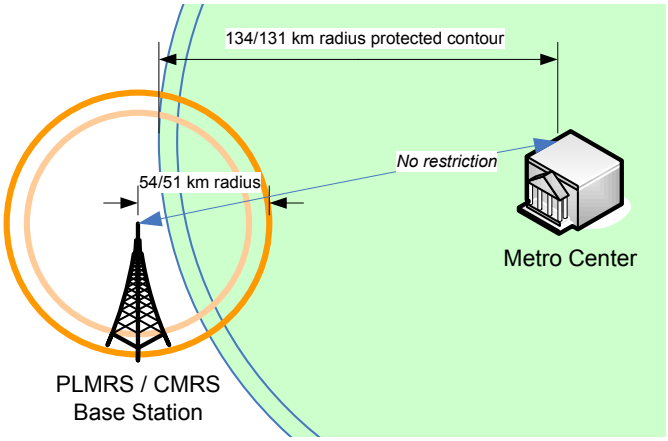


Figure 34: PLMRS and CMRS operate on one or two channels in 13 metropolitan areas. The protected contour is a circle of fixed radius, potentially extended in certain circumstances.

For PLMRS/CMRS base stations located less than 76 km from their metropolitan center no additional analysis is required as the base station's 54 km radius is entirely contained within the metropolitan's protected contour.

For PLMRS/CMRS base stations located greater than 76 km from their respective metro-center the Database will add a second set of 54/51 km radius protected contours centered on the base station location. The net protected contour will be the union of these two circles.

4.6.6.6 Calculating Offshore Radiotelephone Contours

47 CFR §74.712(e) and §74.709(e) describe four geographic contours in the US Gulf of Mexico with protection for channels 15, 16, 17 and 18. These contours are illustrated in Figure 35.

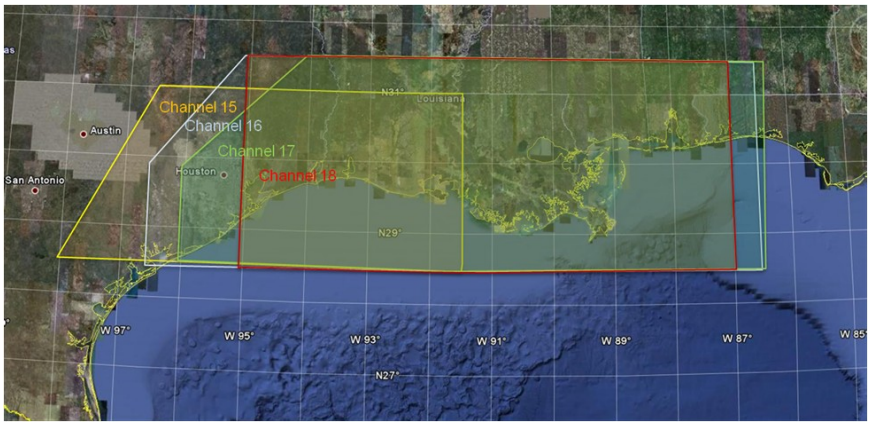


Figure 35: Map illustrating the geographic protection allotted to offshore radiotelephone services in the Gulf of Mexico

4.6.6.7 Calculating Low Power Auxiliary Contours

As described in 4.6.2.3, low power auxiliary services, including wireless microphones (LPAUX), are entitled to one or more circular protected contours each with a fixed radius of 1 km for protection from fixed TVBDs and a fixed radius of 400 meters from personal / portable TVBDs. If multiple reserved contours are made an extended contour is interpolated between points as described.

The LP-AUX protection algorithm first examines whether a simple or complex geometry is present. If the reservation is simple then geographic protection is a matter of determining the separation distance between the inquiring TVBD and the registered LP-AUX device. If the reservation geometry is complex the protection algorithm creates an irregular, convex two-dimensional polygon from the reservation geometry and tests whether the inquiring TVBD location coordinates are inside or outside of the polygon.

4.6.6.8 Calculating Border Areas Contours

US-Canada Border

The International Boundary Commission is a permanent organization responsible for surveying and mapping the US-Canada boundary, maintaining boundary monuments (and buoys where applicable), and keeping the boundary clear of brush and vegetation.

The US-Canada border is defined by 11,522 geographic marker points spanning 8,891 kilometers (5,525 mi) and separated into 18 regional sections. These are:

1. Gulf of Maine (Nova Scotia/Maine)
2. Passamaquoddy Bay (New Brunswick/Maine)
3. St. Croix River (New Brunswick/Maine)
4. North Line (New Brunswick/Maine)
5. St. John and St. Francis Rivers (New Brunswick, Quebec/Maine
6. Southwest and South Lines (Quebec/Maine
7. Southwest Branch of the St. John River (Quebec/Maine
8. Highlands (Quebec/Maine
9. Halls Stream (Quebec/New Hampshire
10. 45th Parallel (Vermont, New York/Quebec
11. St. Lawrence and Great Lakes (New York, Pensylvania, Ohio, Michigan/Ontario)
12. Lake of the Woods to Lake Superior (Minnesota/Ontario, Manitoba)
13. 49th Parallel (Minnesota, North Dakota, Montana, Idaho
14. Washington/Manitoba, Saskatchewan, Alberta, British Columbia)
15. Straits of Georgia (Washington/British Columbia)
16. Portland Canal (Alaska/British Columbia)
17. Southeast Alaska (Alaska/British Columbia)

18. 141st Meridian (Alaska/Yukon)

The Key Bridge TV bands database establishes protection within the US-Canada border on a section-by-section basis as illustrated in **Error! Reference source not found.** and described below:

- Each border section is enclosed within a bounding rectangle
- If the inquiring TV band device is located within the bounding rectangle a closer inspection is made
- A geometric line is constructed from the border section's coordinates
- Finally, the module tests whether the inquiring TVBD is located within the boundaries of the United States

US-Mexico Border

The International Boundary and Water Commission is a permanent treaty organization responsible for administering the many boundary and water-rights treaties and agreements between the two nations.

The US-Mexico border is defined by 236 fixed geographic marker points plus geometry that traces the Rio Grande River. The border spans 3,169 km (1,969 miles) and ranges from San Diego, California in the West to El Paso, Texas, in the East, then from El Paso, Texas along the Rio Grande River to the Gulf of Mexico.

The Key Bridge TV bands database protected the US-Mexico border in two sections as follows:

- The fixed geometric markers between San Diego, California and El Paso, Texas are enclosed within a bounding rectangle

- If the inquiring TV band device is located within the bounding rectangle a second inspection is made similar to the process for the US-Canada border
- A similar procedure is followed for coordinates defining the Rio Grande River

4.6.6.9 Calculating Radio Astronomy Contours

For each enumerated site in the table below a separation distance of 2.4 km is provided for TVBD operation. For the Very Large Array (VLA) an irregular convex polygon is established and the Key Bridge system tests whether the inquiring TVBD location coordinates are inside or outside of the polygon.

Observatory	Longitude (deg/min/sec)	Latitude (deg/min/sec)
Radio Astronomy Observatories		
Allen Telescope Array	121°28'24" W	40°49'04" N
Arecibo Observatory	066°45'11" W	18°20'46" N
Green Bank Telescope (GBT)	079°50'24" W	38°25'59" N
Very Large Array (VLA)	Rectangle between latitudes 33°58'22" N and 34°14'56" N, and longitudes 107°24'40" W and 107°48'22" W	
Very Long Baseline Array (VLBA) Stations:		
Brewster, WA	119°40'55" W	48°07'53" N
Ft. Davis, TX	103°56'39" W	30°38'06" N

Hancock, NH	071°59'12" W	42°56'01" N
Kitt Peak, AZ	111°36'42" W	31°57'22" N
Los Alamos, NM	106°14'42" W	35°46'30" N
Mauna Kea, HI	155°27'29" W	19°48'16" N
N. Liberty, IA	091°34'26" W	41°46'17" N
Owens Valley, CA	118°16'34" W	37°13'54" N
Pie Town, AZ	108°07'07" W	34°18'04" N
St. Croix, VI	064°35'03" W	17°45'31" N

4.6.7 Calculating Available Channels

The Key Bridge channel list query responder is a modular Web services engine that accepts channel list inquiries via the Internet. Incoming requests are first examined for type and content verification to prevent unauthorized access or security breach.

The Key Bridge Equipment Authorization Service ("EAS")[20] is employed to verify the inquiring device's certification status. The inquiring message and verification results are immediately logged.

If the EAS response is negative the device is considered "Not FCC Certified for Unlicensed Operation in the TV Broadcast Bands". A channel list message is constructed with the relevant error conditions and returned to the client. The transaction is then closed.

[20] See 4.6.1.4, *Equipment Authorization*

If the EAS response is positive the device is considered "FCC Certified for Unlicensed Operation in the TV Broadcast Bands". The inquiring device's identifying information is evaluated and, following a successful security check, appropriate channel availability is determined at the device's location.

A high-level representation of the process is illustrated in Figure 36.

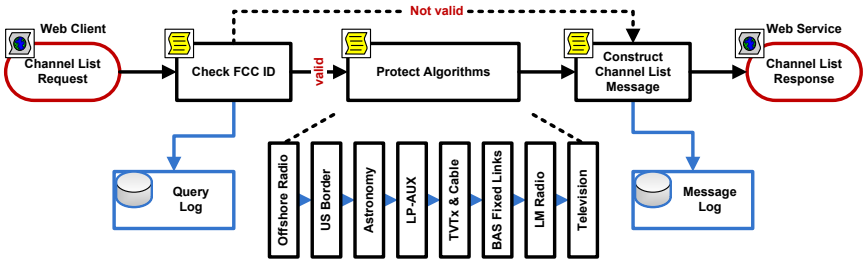


Figure 36: Functional block diagram showing modular design of the Key Bridge solution

All channel list queries and system responses are permanently recorded in a query and message log, respectively, to allow for detailed information reporting, troubleshooting and quality assurance.

Each protection algorithm in the Key Bridge system is an independently developed and operated software program. The software system is designed to accommodate evolution and optimization with growth. Because protection modules operate independently, new modules may be easily inserted and existing modules may be modified, removed, or replaced without affecting the operation of the other modules. This flexibility enables Key Bridge to readily accommodate future changes in TV bands Rules or policy the FCC may require for the analysis of broadcast services and the protection of primary and secondary spectrum users.

4.6.7.1 Channel List Message Structure and Syntax

A standardized message format for TVBD query and response is required. In keeping with industry best practice, such messages should lend themselves to simple storage, indexing, search and retrieval. Messages should also be human readable, self-explanatory and contextually complete (atomic). The Key Bridge proposed channel-list message structure and syntax satisfies best practice requirements including:

- Machine-readable
- Human-readable
- Contextually complete
- Easily indexed

Channel list message data must be formatted, encapsulated and uniquely labeled for easy automatic parsing and software decoding. Messages must also be legible, clearly labeled and self-explanatory for human readability and comprehension. Because messages will be individually logged, message content must be self contained and not require other messages for completeness. Finally, each message must include globally unique identifying information (i.e. a serial number) and a time stamp for later search and retrieval.

The Key Bridge channel-list message structure fully accommodates FCC requirements and is easily extended to support future international TV Band initiatives. Channel lists indicate which modes of operation are allowed on each available channels and provide contextual information for channels are not available.

Incorporated into standard web service protocols is a mechanism whereby the client (TVBD) and server (Database) may negotiate certain transaction parameters. The Key Bridge solution allows TV band devices to specify their preferred message encapsulation and encryption formats.

Actual message structure and content are still under development. However, certain aspects and options are established. The channel list request message structure may contain the fields listed below in Table 1.

Field	Type	Notes
Required Fields		
Request Timestamp	varchar	RFC 3339 encoded date and time when request was submitted
Device ID	varchar	Device FCC ID (US) or International Equivalent
Device SN	varchar	Device manufacturer serial number or equivalent
Device Location	varchar	RFC 5870 encoded latitude, longitude, altitude, datum
Antenna Height	double	The antenna height above ground (m)
Optional Fields		
Device Type	varchar	The device type, possibly required for non-US operation
Account Number	varchar	Commercial account information
Service Type	tbd	The service this device intends to operate (e.g. video, broadband IP, scada, etc.)

Service Mode	tbd	The intended device service mode (e.g. fixed, transportable, mobile)
Optional Channel Request: Repeat for 0 to Max value		
Channel Number	integer(s)	A list of preferred channel(s) this device wishes to operate on
Optional Sensor Data: Repeat for 0 to Max value		
Sensor Data	tbd	Information describing this device's measured RF environment
Alternative Frequency List: Repeat for 0 to Max value		
Desired Frequency	double(s)	Desired operating center frequency or frequencies
Desired Ch. Width	double	Desired operating channel width
Optional Developer Extensions		
Developer Code	tbd	Extension allowing for development and debugging

Table 1: Enumeration and description of various fields in a TVBD channel list request.

Key Bridge's proposed open message structure is easily extended by embedding user-defined fields within the "Optional" field as required.

Key Bridge incorporated Rules requirements plus the many recommendations established in 802.22 and other ongoing efforts and international white space considerations to establish suitable options for a channel list message response as shown in Table 2.

Field	Type	Notes

Required Fields

Create Timestamp	varchar	RFC 3339 - when this channel list was created
Expire Timestamp	varchar	RFC 3339 - when this channel list expires
Message SN	varchar	Message serial number
Device ID	varchar	FCC ID (US) or Equivalent
Device SN	varchar	Device serial number
Device Location	varchar	RFC 5870 encoded latitude, longitude, altitude, datum

Required Channel List: Repeat for 0 to Max value

Available Channels	integer(s)	List of allowed TV channels
Start Time	varchar	RFC 3339 - when a channel may become available
Stop Time	varchar	RFC 3339 - when a channel may become unvailable

Alternate Required Channel List: Repeat for 0 to Max value

Available Channels	integer(s)	List of allowed TV channels
Availability Schedule	varchar	draft-daboo-et-al-icalendar-in-xml-07, XML encoded RFC 5545 iCalendar object describing when a channel may become available and unavailable

Alternate Required Frequency List: Repeat for 0 to Max value

Available Frequency	double(s)	Available center frequency or frequencies (MHz)

Upper Frequency	double	Channel upper frequency (MHz)
Lower Frequency	double	Channel lower frequency (MHz)
Max ERP	double	Maximum allowable ERP (dBm) on the indicated frequency
Adjacent Ch. Mask	double	Adjcent channel mask (dB) below relative Tx power
Optional Developer Extensions		
Error Code	tbd	Extension allowing for development and debugging

Table 2: Enumeration and description of various fields in a TV Bands Database response to TVBD channel list request.

4.6.7.2 Building a Proper Channel List Message

As shown in Figure 36, the Key Bridge TV band solution employs a sequence of independent software modules to determine if a TVBD inquiry is within the service contour of each class of protected entity. The flexible and straightforward process of calculating channel lists is illustrated in fig x and describe below.

Figure 37: The process of creating channel lists begins with a device-specific template. Protected entity tests mask out unavailable channels. A valid, authentic channel list message is constructed, encrypted and signed. In the example shown, message formatting is XML and encrypted information and keys are highlighted in red.

Creating a channel list begins when a TV band device submits its identifying and location information. A new channel list template is created specific to inquiring device type. Presently only two templates are allowed: Fixed or Mode-II.

The channel list template is created with all channels marked “available” for the respective device type. Each protection module then sequentially updates the channel list, inserting protected entity status indicators and masking their respective channels as unavailable.

Following the protection sequence, the channel list is encapsulated into a properly formatted message structure according to the adopted specification.

Finally, message content is encrypted and the message cryptographically signed according to Database policy and the device’s indicated capability.

4.6.7.3 Optional: Frequency Lists versus Channel Lists

The Key Bridge proposed channel list message structure accommodates the default white space spectrum channelization of 6 MHz. To accommodate white space extension into other spectrum bands and possible sub-channelization within the Television broadcast bands Key Bridge may support TVBD requests for preferred operating frequencies and channel widths. The respective database response may in turn indicate available frequencies (instead of channel) and sub-channel operating parameters.

4.6.7.4 Optional: Channel List Message Codes

Channel lists are encoded as custom formatted ASCII sentences following the NMEA grammar format. They include a four character header followed by a channel list character sequence of arbitrary length limited to maximum 256 characters. The Headers may be extended to accommodate future enhancements.

Channel lists in the US are 51 characters long.

Each character in the sentence encodes the respective channel availability at that character's position. For example, the US character sentence is 51 characters long, corresponding to 51 channels. The character in position for channel 1 always indicates "Not available."

NMEA sentences begin with a dollar sign. The sentence header is therefore "$CHAN" for channel list.

Numbered channel codes indicate the allowed modes of operation and characters indicate reasons why a channel is not available:

- [1-9] YES codes indicate operation is allowed with restrictions
- [0, A-Z] NO codes indicate operation is not allowed for the identified reason

List of Channel List Message Codes

Code	Available	Description
0	NO	Prohibited
1	YES	<= 100 mW
2	YES	<= 40 mW
3	YES	<= 4 W
4	Reserved	
5	Reserved	
6	Reserved	
7	Reserved	
8	Reserved	
9	YES	Variable Power – Check MaxERP field for the value
A	NO	Channels 3,4 are not available in the US
B	NO	Mode-II operation is not allowed under Ch. 20
C	NO	Offshore Radiotelephone Service Channels 15-18
D	NO	Not within legal geography (e.g. United States and territories)
E	NO	
F	NO	
G	NO	Radio Astronomy

H	NO	Television: Fixed Operation within Co-Channel Contour
I	NO	Television: Fixed Operation within Adjacent Channel Contour
J	NO	Television: Mode-II Operation within Co-Channel Contour
K	NO	Television: Mode-II Operation within Adjacent Channel Contour
L	NO	TX/MVPD Receive: Operation within Co-Channel Contour
M	NO	TX/MVPD Receive: Operation within Adjacent Channel Contour
N	NO	Fixed Bas Link: Operation within Co-Channel Contour
O	NO	Fixed Bas Link: Operation within Adjacent Channel Contour
P	NO	LM Radio: Operation within Metro Center Co-Channel
Q	NO	LM Radio: Operation within Metro Center Adj-Channel
R	NO	LM Radio: Operation within Waiver Site Co-Channel
S	NO	LM Radio: Operation within Waiver Site Adj-Channel
T	NO	LP-AUX: Operation within Co-Channel Contour
U	Reserved	
V	Reserved	
W	Reserved	
X	Reserved	
Y	Reserved	
Z	Reserved	

4.6.7.5 Optional: Late Start and Short Lease Channel Lists

FCC rules describe a radio resource coordinator (TV bands database) that makes channels available for or precluded from unlicensed use in 24-hour increments. This creates a number of inefficiencies and limitations for secondary users. As an example, wireless microphones may operate for short periods while any microphone activity on a given channel during a 24 hour period may render that channel unavailable for the entire 24 hours.

IEEE 802.22, a proposed standard for Wireless Regional Area Network (WRAN) using TV band white spaces, provides a channel list message structure that incorporates an "availability schedule" containing a start and stop date/time for each channel [21]. 802.22 does not accommodate "overtime" scenarios where protected users may require unscheduled reservation extensions.

Increased unlicensed channel availability may be possible if "late start" and "short lease" concepts incorporate a "reservation release" mechanism for protected users.

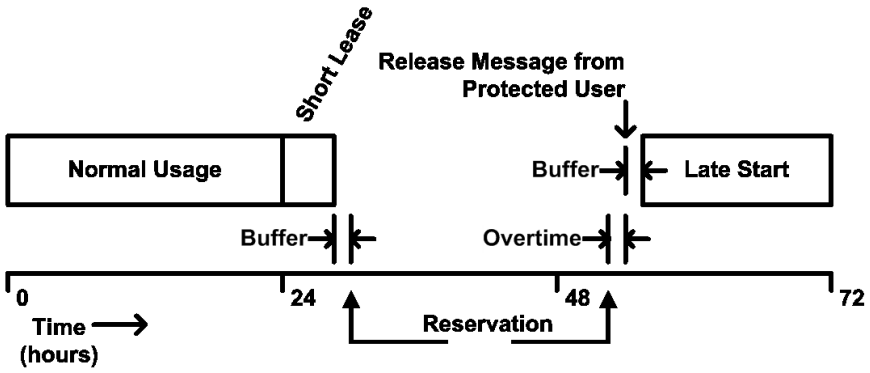


Figure 38: Late-start & short-lease channel list concept

[21] See IEEE 802.22-09/00123R13 page 6

"Short lease" describes channel availability at a normal start time but only for the specified duration. The duration instructs a secondary user (TVBD) that channel availability will end shortly before the primary user's reservation begins. A time buffer is incorporated to facilitate TVBD channel evacuation.

"Late-start" indicates that a channel is not available at the time of inquiry but may become available within the current 24-hour period. Late start does not mean the channel is available. Rather, the TVBD is invited to re-inquire about the channel's availability at the indicated time.

When combined, both methods enable "late-start plus short-lease" windows.

Overtime is accommodated with a "Release Message" from the protected user indicating the conclusion of their reservation to the TV Bands Database. If no release message is received, the reservation will expire normally (at the 24 hour mark). An optional (but not necessary) time buffer may be added if desired.

The Key Bridge channel list message structure accommodates "Short Lease/Late Start" operation.

4.6.8 Key Bridge Un-bundled TV Bands Services

TV Bands White Spaces offer an unprecedented opportunity for innovation in unlicensed wireless products and broadband services. However, businesses wishing to provide innovative TV Band services must provide end-to-end solutions.

As a neutral TV Bands database administrator, Key Bridge may offer unbundled White Space services to other FCC authorized service providers on a non-discriminatory basis.

Key Bridge unbundled TV Band services may be offered to other FCC designated administrators on a non-discriminatory basis. Unbundled TV Band services present a secure and affordable

foundation upon which businesses can build innovative White Space services while assuring FCC rules compliance.

4.6.8.1 Channel List Calculations

Key Bridge has an open channel list structure that meets present FCC requirements. It is secure, robust and extensible to accommodate future FCC requirements and international TV Band initiatives.

Our channel list messages include extensive contextual information for service providers and spectrum managers, such as detailed YES/NO codes and developer extensions. Key Bridge also accommodates client-specified message encapsulation (XML, JSON, HTML, NMEA text, etc.), providing maximum flexibility for service providers and device manufacturers.

4.6.8.2 Equipment Authorization

Key Bridge unbundled equipment authorization service provides assurance that inquiring devices are both FCC certified and authorized to operate as an unlicensed TV band device.

As with our channel lists, authorization messages contain extensive contextual information for service providers and end-users including:

- Manufacturer
- Certification date
- Allowed frequencies and channels
- Possible service restrictions

4.6.8.3 Equipment Registration and Records Verification

Broadcast locations like wireless microphones and cable head ends must register to receive protection, while incumbents will want to confirm their broadcast facilities and service area records are correct.

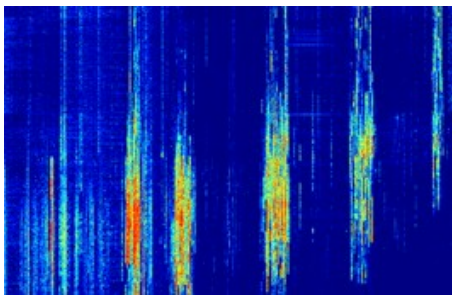
Key Bridge provides a secure developer API for businesses to streamline and automate these processes.

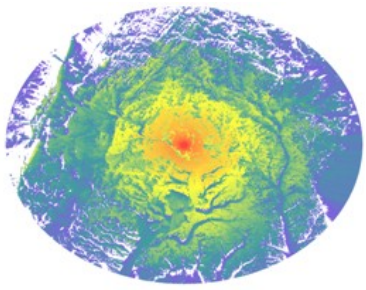
- Register entities, devices & events
- Confirm facilities and contours
- Streamline records management

4.6.8.4 Enhanced Information Services

Key Bridge enhanced information services provide additional valuable context when deploying or troubleshooting unlicensed wireless services. We provide signal analysis data and can feed into various mapping applications.

- Geo-coded transmitters
- Geo-coded service contour geometries
- Signal propagation analysis
- Field strength estimates and measurements





5 Security Strategy

The Key Bridge solution team includes Fortinet, a leading provider of network security appliances and the leading provider of unified threat management (UTM) solutions worldwide, and Symantec, the largest maker of security software for computers, the largest provider of embedded cryptographic digital certificates and the largest operator of public key infrastructure. Together, the Key Bridge Team offers a comprehensive security solution for protecting the TV bands database ecosystem.

Database system reliability, authenticity and availability are critically important for the successful operation of unlicensed devices in the TV bands. Incumbent operators will rely upon the Database to ensure their continued and uninterrupted business operation, while new wireless service providers will be operationally dependent upon accurate channel lists.

The TV band ecosystem will face similar threats to other wide-area Internet systems and services. Key Bridge and Fortinet have combined our years of operational experience and best practices to design a robust, secure TV bands service infrastructure that will meet the Commission's highest expectations.

Our TV bands database solution addresses all of the known system threats with a standards compliant security framework that provides robust message security, information assurance, mutual authentication and non-repudiation.

Fortinet's hardware-based security solutions integrate multiple levels of protection including firewall, virtual private networking, antivirus, intrusion prevention, Web filtering, anti-spam and wide area network (WAN) acceleration. Fortinet provides the Key Bridge solution with integrated protection against dynamic security threats.

Symantec, through its acquisition of VeriSign Security, provides Secure Sockets Layer (SSL) Certificate Services, the Public Key Infrastructure (PKI) Services, the VeriSign Trust Services and the VeriSign Identity Protection (VIP) Authentication Service. Symantec provides the Key Bridge solution with strong identity and authentication services with integrated capabilities for fraud detection plus identity and robust protection for confidential or sensitive information.

5.1 Protecting the TV Bands Ecosystem

A Security Domain is an enclave of computer applications that are functionally distinct. Within a security domain, applications are typically configured to trust one another and may freely communicate. In a networked environment, different security domains are isolated behind firewalls and only allowed to communicate with other domains via designated methods.

The TV bands ecosystem can be modeled as three aggregate security domain, each containing multiple enclaves. These are shown in Figure 39 and are the Administrator Domain, the Internet Domain and the Client Domain.

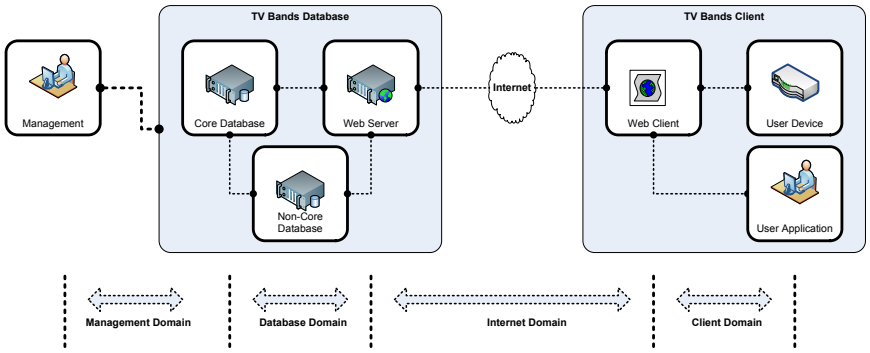


Figure 39: Direct communications are only allowed within a domain. Each domain has a unique threat profile and corresponding security framework. Secure end-to-end information exchange from the database to user devices is enabled by authenticated messaging through mediating web servers and web clients.

The Database Domain contains all of the TV bands database system enclaves. These are consolidated into three sub-domains:

- Core Database
- Non-Core Database
- Web Server

The Core Database enclave contains the TV bands Master database computer clusters running Oracle RAC. It is the heart and central data repository of the TV bands system.

The Non-Core Database enclave contains all of the supporting databases running clustered or single instances of MySQL. The Non-Core Database enclave consists of several isolated sub-enclaves including the staging systems for data import and exported instances for inter-Database synchronization

The Web Server enclave encapsulates all of the system's computers that provide the various Web services and Web portals. As shown in Figure 39, only the Web Server enclave is allowed to communicate with the Internet Domain.

The Client Domain represents all of the allowed TV band client functionality and has three sub-domains:

- Web Client
- User Device
- User Application

The Web Client enclave is a standards-compliant Web services client that supports the minimum transport-layer encryption required to communicate securely with the Web Server enclave.

Together a Web client and Web server application, operating within their respective security enclaves, provide secure and assured message communications across the Internet Domain.

The User Device enclave contains the all of the functionality of a TV band device except for the web client. In practice, user device applications exchange messages with the Web Server enclave via a Web client, which provides client-side authentication, encryption and message transport.

The User Application enclave provides a formally defined security profile for user applications to interface directly with the TV Bands Database via Web services.

5.2 Protecting the TV Bands Database System

The TV bands database system is modeled with three security enclaves. The Key Bridge / Fortinet / Symantec security strategy employs functional isolation and logical segmentation to prevent unauthorized access, protect sensitive data and limit the potential effect of a system breach, attack or failure.

Functional isolation is a system security technique that groups applications and computer systems with similar functionality and security threats profiles into a dedicated security enclave. It allows the application of tailored security profiles to counter known threats and limit the possible impact of unknown threats.

Logical segmentation supervises resource availability for applications. Logical segmentation creates security communities across system components without regard to their physical location. It creates a flexible, layered security approach based on applications, application groups, IP addresses and geographic regions and allows the creation and application of tailored security profiles to isolated Web service modules and computer systems.

Logical segmentation has several key benefits, principal among them the ability to pinpoint and prevent attacks at a very fine level. It provides a robust method to prevent "pivot" attacks, where one compromised service is exploited to attack others.

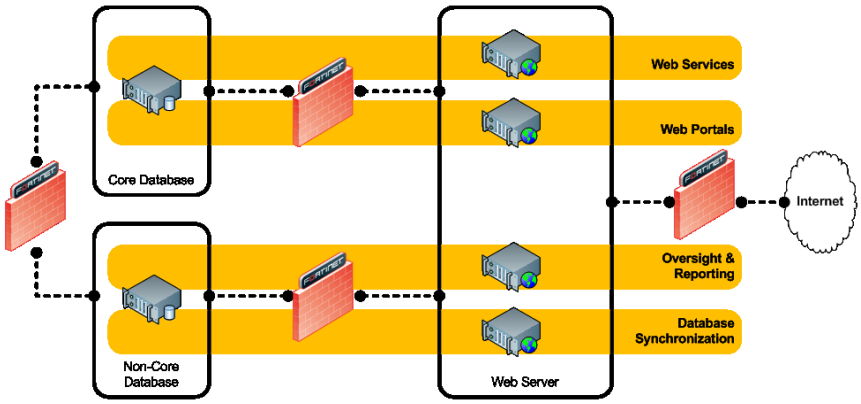


Figure 40: Illustration of physical connectivity and functional plus logical security groupings for the database applications listed on the right. Firewalls strategically located between systems provide fine-grained application of tailored security profiles.

The Key Bridge solution enforces a positive security model. Our solution has tremendous flexibility in this respect. As illustrated in Figure 40, it accommodates data security at the physical and logical networking layers, in between security enclaves, and the application components of system applications.

5.2.1 Protecting the Core Database Enclave

The TV bands Master database is four geographically distributed computer clusters configured in a logical mesh: three physical installations and one virtual installation within a cloud compute environment. Database nodes are continually synchronized with each other in near real-time, providing geographic load balancing and fail-over. This is illustrated in Figure 41.

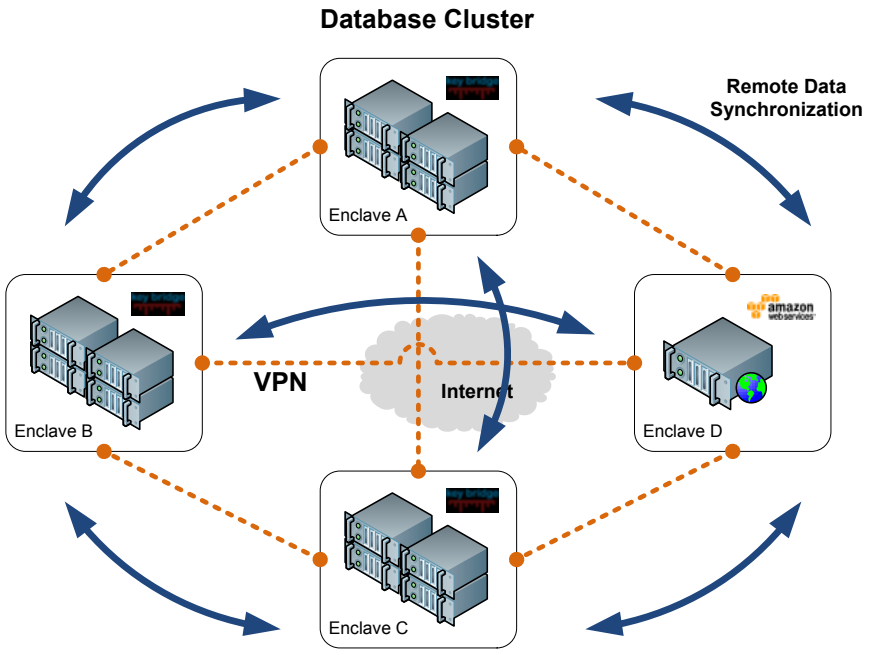


Figure 41: The Key Bridge Core TV bands database consists of four high-availability computer clusters in constant synchronization. Each node provides load sharing and failover or backup capability to the others.

Each individual computer cluster is protected in a security enclave. Only administrative database communications like data synchronization, load balancing and failover are allowed between enclaves. Enforcing limited trust between nodes serves to limit the system-wide impact of potential operator error or security breach.

5.2.2 Security Management and System Auditing

A new Management security enclave is created to allow system management and auditing. The Management enclave is logically attached to various TV Bands Database enclaves. As shown in Logical attachments are configured to allow data query, logging and auditing messages between enclaves in the Management domain and the Administrator domain.

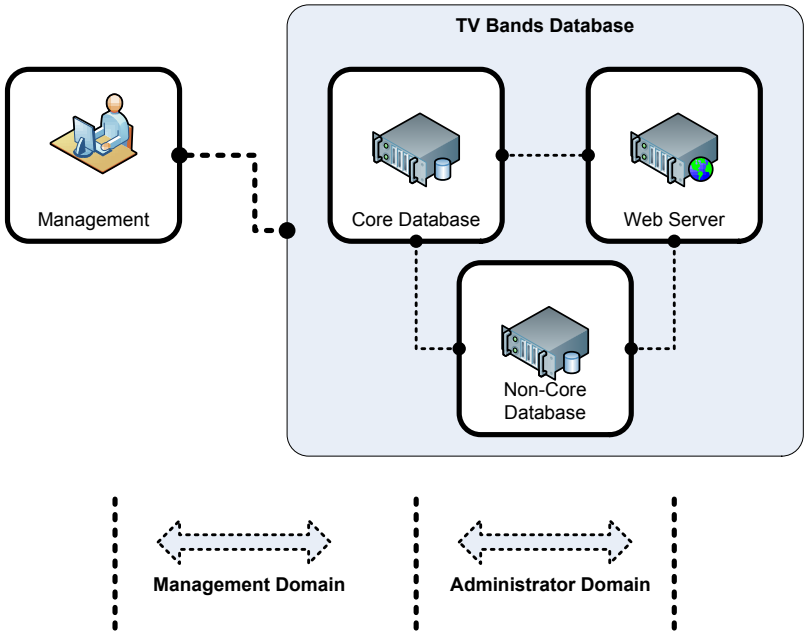


Figure 42: A management enclave attaches to others in the Administrator Domain to receive logging data and is allowed to execute status inquiries against the various systems.

The Key Bridge solution leverages standards-compliant functionality in Fortinet and Symantec's respective products and services to allow secure logging, auditing and device management between the Management enclave and other enclaves within the TV Bands database. In Figure 42 each connection between enclaves represents a security policy enforcement point. The principal is to enforce granular control of applications and message traffic, pinpoint anomalies, and to prevent any undesired activity either from internal misconfiguration or malicious act.

The Keybridge / Fortinet / Symantec solution may also utilize Fortinet's FortiDB product suite for auditing and vulnerability protection. FortiDB continuously monitors the Key Bridge databases, looking for suspicious or abnormal activity and providing Key Bridge operations personnel with an early warning of potential malicious activity. Continuous vulnerability assessments regularly scan the database servers to ensure they are patched for any known vulnerabilities to the database server software.

5.3 Protecting TV Band Devices

A valid FCC ID and serial number are required to communicate with the Database. Combined with a public/private cryptographic key, the FCC ID and serial number constitute a complete set of credentials that enable a device to both connect with and authenticate itself to the Database. Once authenticated with the system, TVBDs may access any authorized Database service and data.

While the Rules require that TVBDs must directly access a Database, there exists a real risk that an unauthorized Database could provide Internet-based channel list services to unsuspecting or intentionally mis-configured TV band devices. Unauthorized databases cannot have a complete or current set of protected service records and the devices they serve would be very likely to cause harmful interference with incumbent protected services.

Furthermore, unauthorized Databases undermine the FCC's device certification requirement and negate the Commission's TV band enforcement capability. Because they disable network management and interference protection, unauthorized databases represent a significant operational and commercial risk for protected broadcast operations and valid unlicensed TV band services alike. Unauthorized databases are a serious and fundamental risk to successful unlicensed operation in the TV bands.

- A party could set up and operate an unauthorized but technically valid Database service
- A party could intercept connections and represents itself as a Database (man-in-the-middle)
- End users could purposefully misconfigure their devices to access an unauthorized Database

Most unauthorized Database risks are addressed when TV band devices only connect and accept channel lists from an authentic Database. Key Bridge, Fortinet and Symantec have designed a security solution that is robust scalable and standards complaint. It protects TV band devices

from man-in-the-middle attached, phishing schemes, hacking and other unwanted scenarios with mutual authentication, transport security, message signatures and data encryption.

Transport encryption addresses the risk of data interception. The Key Bridge / Fortinet / Symantec solution only allows connections to between IP hosts that present valid credentials. Unless the intercepting party has stolen the licensed Database private keys without the Database's awareness (an exceedingly difficult task), a hijacked or intercepted connection would be immediately recognized by the TV band device.

The Key Bridge / Fortinet / Symantec solution employs transport layer security with public key infrastrucutre (TLS-PKI). TLS-PKI provides for secure communication using a public key infrastructure, where pre-shared root certificates may be exchanged in advance at the time of device registration.[22] The Key Bridge solution leverages the Symantec public key infrastructure for key exchange.

With mutual authentication TVBDs and the Database may establish a connection only after authenticating each other. Both systems may then be reasonably (but not absolutely) assured of the other's identity. Mutual Authentication helps to address two important operational requirements for successful unlicensed TV band operation:

- Only authorized devices may connect to a Database
- All devices must only connect to and receive channel lists from a licensed Database

[22] See 4.6.4, *TV Band Device Registration*

An important concept in mutual authentication is that neither party should "trust" the other until their identity has been proven. Public key infrastructure means that the server may determine who clients are without asking the client and clients may determine who the server is without asking the server. With mutual authentication, it is difficult to compromised security through impersonation.

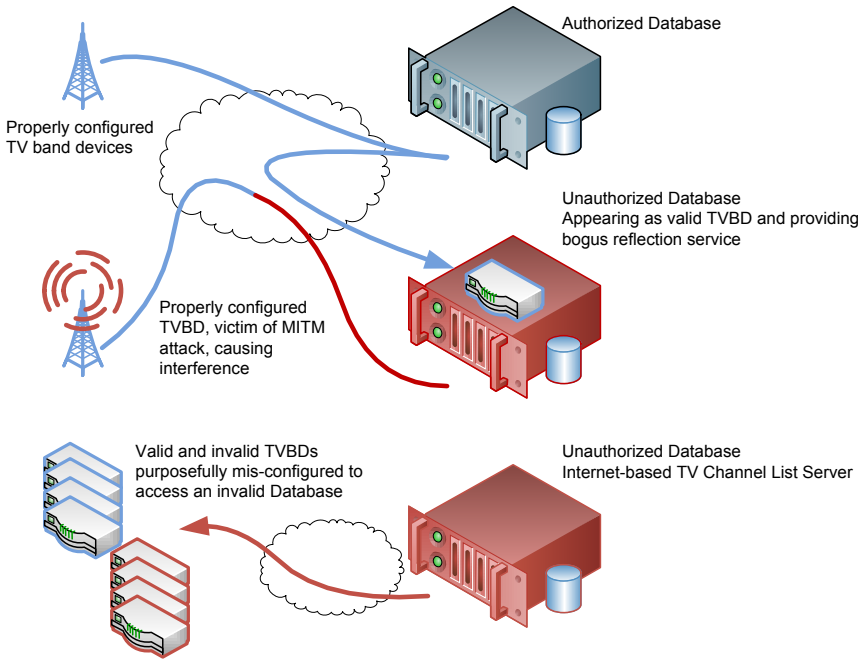


Figure 43: Unauthorized Databases present a more serious set of risks as they enable misconfigured TVBDs to evade FCC certification and enforcement. At best such devices could disrupt protected services and at worst cause widespread purposeful TV band interference.

5.4 Protecting Application Services

Messages received from the Internet cannot be trusted by default, and the Key Bridge TV bands database solution employs several procedures and technologies to ensure system security. These include:

- Only authorized TVBDs may connect to the Database
- TV band devices and the Database must employ mutual authentication
- Insecure communications are not allowed between TVBDs and the Database
- All communications with the database must be protected by Transport Layer Security (TLS) or IPSEC
- Messages must have end-to-end protection with WS-Security's authentication, integrity and confidentiality procedures

The Key Bridge / Fortinet / Symantec security solution employs a hardware-based network concentrator which is Common Criteria EAL4+ and FIPS 140-2 Level 2 certified to allow assured communications between the Web Server and TV Band client security enclaves. All communication sessions are authenticated, encrypted and directed to their appropriate application destination depending upon type of TV band client. This is illustrated in Figure 44. Either Transport Layer Security (TLS) or IPSEC provides secure communications, depending upon the capabilities and configuration of the TV band client.

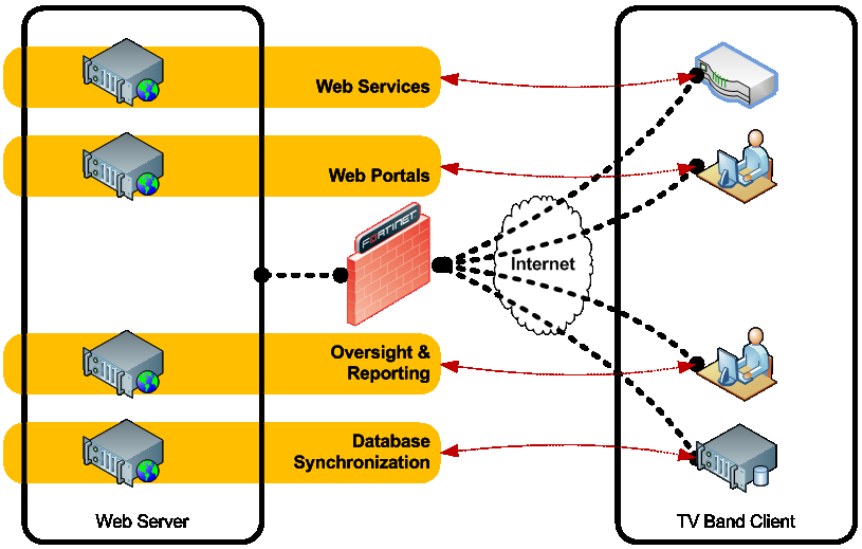


Figure 44: A high-availability cluster of VPN concentrators protect Internet domain transactions. The system provides authentication and secure communication between TV band clients and their respective TV band database service.

All communication with the TV bands database is via secure Web services, which provide interoperable protocols for Security, Reliable Messaging, and Transactions in loosely coupled systems. As background, a Web service is a self-contained, self-describing modular application published, discovered, and invoked over a network using standard protocols. Several open standards fully describe a web service:

- XML (Extensible Markup Language) typically encapsulates data while JSON (JavaScript Object Notation) is growing in popularity
- SOAP (Simple Object Access Protocol) or REST (Representational State Transfer) to transfer the data
- WSDL (Web Services Description Language) described how to interface with a web service

- UDDI (Universal Description, Discovery and Integration) publishes the services for general availability

The Key Bridge solution incorporates a standards compliant implementation of Web Services Security (WS-Security) to protect both client and server applications and enable them to communicate across the Internet Domain.

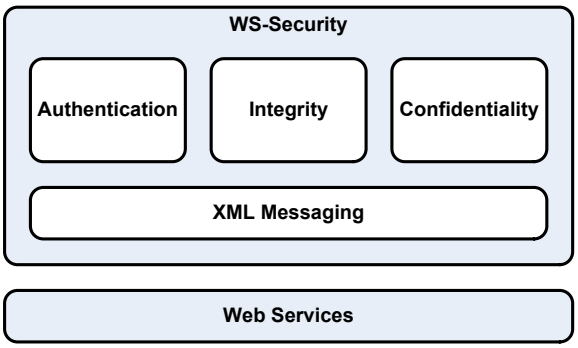


Figure 45: Web Service Security (WS-Security) adds message authentication, integrity and confidentiality to standard Web services.

WS-Security is a formally defined set of procedures and software protocols for securing Web services. The WS-Security specification describes messaging enhancements that provide integrity, confidentiality, and mutual authentication for secure data transactions. The WS-Security protocol was originally developed by IBM, Microsoft, and VeriSign and has become a widely adopted open software standard.

WS-Security provides end-to-end transaction security by incorporating security features directly within messages. It specifies how Web services may offer integrity and confidentiality, how digital signatures may be attached and encrypted data embedded within messages.

The WS-Security specification provides the following three mechanisms for securing Web services at the message level:

- Authentication
- Integrity
- Confidentiality

Authentication uses a security token to validate users and determine whether a client may access a web service. Clients can be end users, machines, applications, or other web services. Without authentication, an attacker can use spoofing techniques to send a modified SOAP message to the service provider.

Integrity uses message signing to ensure that message data is not changed, altered, or lost. Integrity uses XML digital signatures on the contents of SOAP messages. Without integrity, an attacker can use tampering techniques to intercept a SOAP message between the Web service client and server and then modify it.

Confidentiality uses message encryption to ensure that only unauthorized parties with proper access may read message information. Without confidentiality, an attacker can use eavesdropping techniques to intercept a SOAP message and read the contained information.

A dedicated WS-Security solution provides a robust, standards compliant and scalable message security solution that meets the most demanding processing and threat environments.. The Web Service security solution provides protection against known and unknown threats by looking for potential malicious threats such as SQL injection attacks, cross-site scripting (XSS) attacks and attempts to circumvent workflow. It does this by enforcing compliance for all activities outside of the WS application domain.

5.4.1 Message security architecture

The WS-Security message security architecture requires four components to fully describe a web service client and server system with assured messaging. These components are shown in Figure 46 and described below:

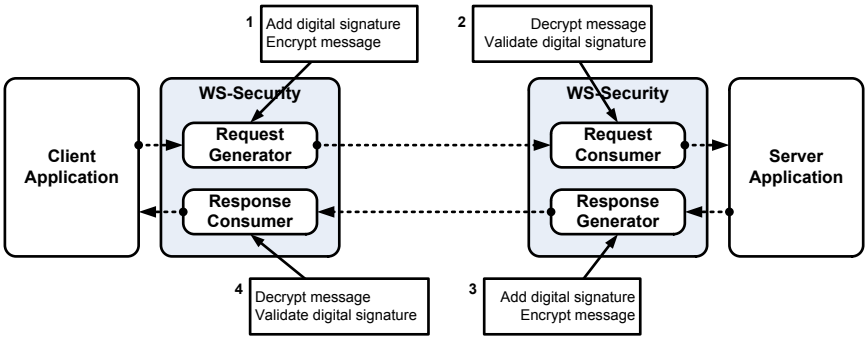


Figure 46: WS-Security message security architecture

	Component	Description
1	Request generator	On the client side, the request generator defines the security constraints on the outgoing request message with one or more security mechanisms, such as digital signing, encryption, or security tokens.
2	Request consumer	On the server side, the request consumer defines the acceptable security constraints on the incoming request message, such as: • The required integrity parts must be signed and the signature is verified • The required confidential parts must be encrypted decrypted • The security tokens are valid The WS-Security properties defined for the request consumer must match

	Component	Description
		those of the request generator.
3	Response generator	On the server side, the response generator defines the security constraints on the outgoing response message with one or more security mechanisms, such as digital signing, encryption, or security tokens.
4	Response consumer	On the client side, the response consumer defines the security constraints on the incoming response message, such as: • The required integrity parts must be signed and the signature is verified • The required confidential parts must be encrypted decrypted • The security tokens are valid The WS-Security properties defined for the response consumer must match those of the response generator.

There are many advantages to using hardware accelerated WS-Security as described in the Key Bridge / Fortinet / Symantec solution. Different parts of a message may be secured separately and according to different security requirements. For example, integrity can be applied to the security token (user ID and password) and confidentiality on the SOAP message body. End-to-end message-level security is assured through any number of intermediary message exchanges. WS-Security works across multiple transports and is independent of the underlying transport protocol and mutual authentication and multiple party authentications are supported.

5.4.2 Message Security Implementation: WS-Security

4.6.7.1: *Channel List Message Structure and Syntax* describes channel list as containing encoded data within an XML formatted message structure. Prior to sending, a digital signature is inserted into the message and the channel list is encrypted.

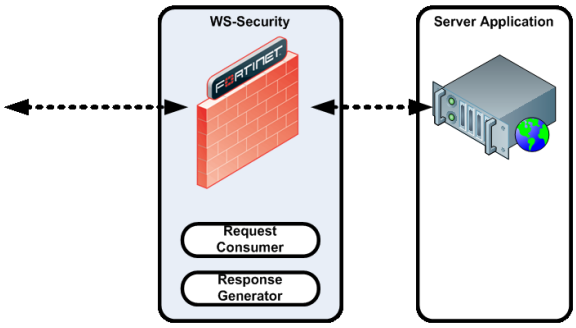


Figure 47: Key Bridge implementation of WS-Security with separation of responsibility. Security configuration and management is established independently of application functionality. This provides robust security, standards compliance and extreme scalability.

The dedicated WS-Security solution provides a robust, standards compliant and scalable message security solution that meets the most demanding processing and threat environments.

5.4.3 WS-Security with TLS or IPSEC

Transport Layer Security (TLS) and IPSEC provide confidentiality and data integrity for Web services. WS-Security combined with TLS or IPSEC enables end-to-end message integrity and confidentiality and addresses several security risks like unauthorized databases, database relays and reflectors.

Transport Layer Security (TLS) is a secure cryptographic protocol for communications over IP networks. TLS is an IETF standards track protocol (RFC 5246) based on SSL that encrypts network connections at the Transport Layer.

IPSEC is a security technology that enables mutual authentication during the establishment of connections between hosts and provides for strong encryption and source authentication of each IP packet exchanged between the connected hosts. Because IPSEC operates at the Network layer of the OSI stack it has a number of important advantages for application development and system operations and scale. IPSEC connections are completely transparent to applications.

5.5 Protecting Sensitive Commercial Information

Voluntary registration data submitted to the TV band database is considered commercially sensitive or proprietary and database administrators must implement a strategy for protecting data at rest.

Within the Key Bridge system records are only available for review by authorized individuals or company representatives. Key Bridge protects sensitive database information from unauthorized access using Oracle Transparent Data Encryption. Most encryption solutions require encryption functions within the application code. This limits modular programming and limits software interoperability. Oracle Transparent Data Encryption deeply embeds encryption in the Oracle database. Application logic work without modification and the Oracle database automatically encrypts data before writing the information to disk.

Key Bridge protects sensitive data during transport (in motion) between systems with strategic use of Fortinet's Fortigate security appliances. Fortigate is a high-performance hardware-based security appliance with a comprehensive array of hardware-accelerated functions including transport layer and real-time message encryption, among others.

All message exchange between internal and external systems is protected with three layered steps:

- Each system is authenticated
- The transport layer is encrypted
- Transaction messages are signed and their sensitive content encrypted

Employing hardware based transport and message encryption enables software applications to focus on functionality without distraction and enables administrators to apply finely tuned security profiles to match each system's threat profile.

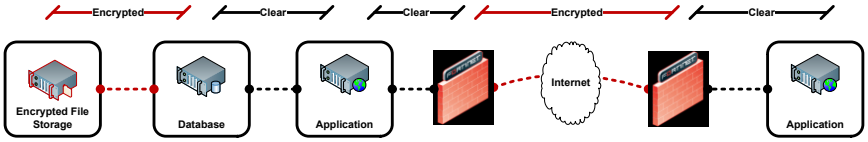


Figure 48: Sensitive data is protected by the strategic application of encryption technologies (Red). Database encryption prevents unauthorized data access through the file system, while network encryption prevents interception. The encryption strategy is transparent to system applications, which focus on functionality.

6 Development, Interoperability Testing, Certification

The Key Bridge proposed TV bands channel lists include several optional fields to accommodate developer testing and database response.

Our solution is built from standards compliant software and hardware components and interoperability testing and certification should be relatively straightforward. To request and consume secure channel list messages from the Key Bridge TV bands database, TV band devices and user applications must only comply with a short, well-defined set of open Internet standards.

The Java Community Process (JCP) specification JSR 109 (Implementing Enterprise Web Services) promotes building portable and interoperable web services in the Java EE environment. JSR 109 leverages Sun J2EE technologies to provide an industry standard for developing and deploying web services. This specification outlines the lifecycle of web services, including how Web clients discover and consume TV band Web services.

JAX-RPC is a Java API for XML-based Remote Procedure Calls (RPC). Key Bridge uses it to build standards-compliant Web services and support any authorized TV band device client that supports RPC and XML.

JAX-RPC uses an XML-based protocol such as SOAP or REST, which defines a message envelope structure, encoding rules, and exchanging RPC messages over HTTP. An advantage of JAX-RPC is that it hides the complexity of XML messaging from the developer and assures interoperability between Web service and Web client. Here is how it works:

- The Web server developer specifies the remote procedures (Web services) that remote clients may invoke and implements the interface using JAX-RPC
- Web client developers create a Web service client using the JAX-RPC software library and then simply invoke the methods on the Web client. A client accesses a Web service using a

Service Endpoint Interface defined by JAX-RPC. The client view of a Web service is the Web server's published set of methods that perform business logic on behalf of the client.

Web server and client developers need not worry about generating or parsing SOAP messages. JAX-RPC handles them transparently during runtime. This allows any JAX-RPC compatible Web client to interoperate with any authorized JAX-RPC compatible Web service.

6.1 Device Testing and Database Certification

Key Bridge provides a development sandbox and documented application programmer interface to Database Web services.

Developer Web services are based on XML-based open standards, such as the Web Services Description Language (WSDL), the Simple Object Access Protocol (SOAP), and Universal Description, Discovery, and Integration (UDDI).

The Key Bridge developer sandbox is a defined, published and interoperable resource for TV band client applications. The development sandbox provides a fully functional instance of the channel list query responder for TV band device software development and testing. The sandbox instance uses a static database for consistency and enables developers to activate or deactivate server-side features to ease client-side application development and testing.

For example, developers may enable or disable extensive debugging output in the NOTES and ERROR channel list fields. They may selectively disable WS-Security procedures, re-order the execution of protection calculation modules, and purposefully inject data errors and security faults into messages.

Figure 49 shows how any JAX-RPC compatible Web client may communicate with the TV bands channel query Web service. Note that the client need not be a Java application. For

example, Web Services Interoperability Technology (WSIT) is an open-source project started by Oracle Inc. that allows developers to create web service clients using Microsoft's Windows Communication Foundation (WCF) and .NET.

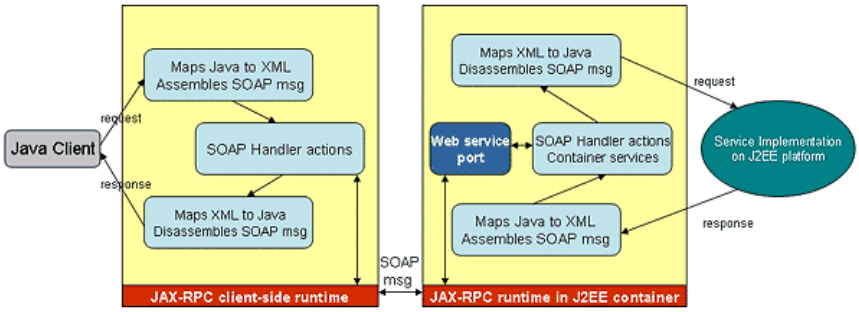


Figure 49: A Java client calling a J2EE web service. The figure would changes only slightly for non-Java clients.

All the messaging details between the request and the response happen behind the scenes.

Key Bridge also provides a series of procedural tests that developers may use to self-certify their applications for each of the interoperability requirement listed above. The tests describe input data, output response, transaction flow and required application actions.

These Key Bridge resources will be available to support the Commission's own TV band device testing and certification efforts.

6.2 Development and Interoperability Standards

For TV Band devices must support the following open Internet standards to successfully communicate with the TV bands database:

- Transport Layer Security (TLS) or IPSEC web client capability
- Certificate-based TLS or IPSEC mutual authentication capability
- Support of JAX-RPC and WS-Security authentication, integrity and confidentiality protocols

Other Database administrators must support the following open Internet standards to successfully synchronize their systems with the Key Bridge TV bands Database:

- Transport Layer Security (TLS) or IPSEC web client capability
- Certificate-based TLS or IPSEC mutual authentication capability
- Support for one or more of the following technologies:
    - JAX-RPC and Java Message Service (JSR 914)
    - MySQL database peering
    - Bulk retrieval via Secure File Transfer Protocol (SFTP)

An unlimited number of individuals may be authorized by the Commission to access the Key Bridge web portal and execute FCC Oversight, Reporting and Enforcement functions. To use the system they must have:

- A web browser that supports HTTPS

Manufacturers, professional installers and end users may register TV band devices either through the Web portal or directly via web service. For web portal access, users must have:

- A web browser that supports HTTPS

For automated, machine-to-machine communication, they must support the following open Internet standards:

- Transport Layer Security (TLS) or IPSEC web client capability
- Certificate-based TLS or IPSEC mutual authentication capability
- Support of JAX-RPC and WS-Security authentication, integrity and confidentiality protocols

For voluntary registration of protected entities like Cable head ends and Microphone devices may use the Web portal and must have:

- A web browser that supports HTTPS

To automate the process and integrate Key Bridge's web services into their back office middleware, the following open Internet standard must be supported:

- Transport Layer Security (TLS) or IPSEC web client capability
- Certificate-based TLS or IPSEC mutual authentication capability
- Support of JAX-RPC and WS-Security authentication, integrity and confidentiality protocols

7 Implementation Plan

The Key Bridge Team has designed a comprehensive solution that provides high performance and high availability secure TV band services on a non-discriminatory basis.

The Key Bridge Team brings more than a decade of experience designing, developing, deploying and operating high performance, high availability Web based applications and infrastructure. Key Bridge staff has a successful history of building and operating vary large information technology solutions, while Team member AWS manages over 800 servers across the country for its own Internet properties including web sites and applications that support over 30 million monthly visitors and over 3 billion transactions per day.

The Key Bridge TV Band solution team has a ready group of management, operations and quality control professionals able and prepared to begin delivering high availability TV band services. The Team has developed a four-stage implementation plan that reflects our assessment of how TV bands devices will be adopted and how the demand for services may evolve. It begins with technology development, standardization, testing and field trials and quickly moves to full-scale Internet deployment.

Implementation begins with a virtual installation, the lowest cost installation, adds up to three physical nodes, and then splits those nodes as necessary to accommodate growth and scale. We have segmented implementation into three distinct phases, zero, one and two, with each having its own schedule, scale and scope of capabilities, and capital requirement.

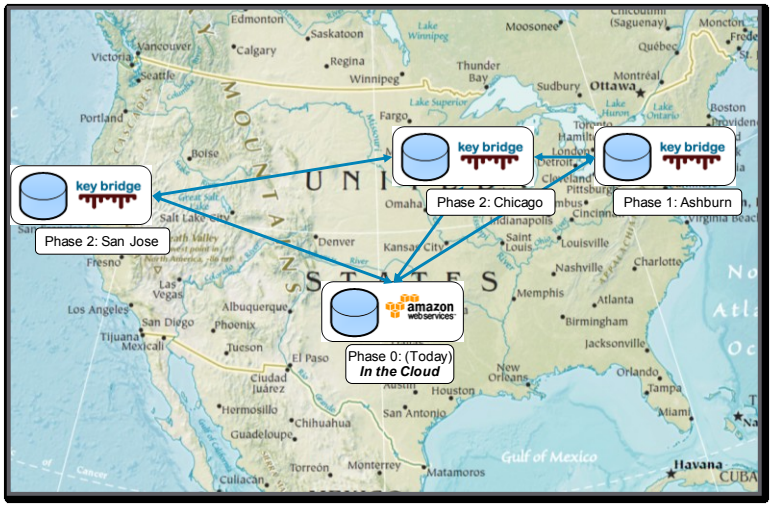


Figure 50: The Key Bridge solution employs geographic and logical diversity to eliminate single points of failure. Implementation begins with a virtual installation, then adds physical nodes for redundancy and scale.

7.1 Phase 0: Development, Testing and Field Trials

In 2009 Key Bridge assembled a solution team to design, develop and deploy a prototype TV band database (Database) instance on the Amazon Elastic Compute Cloud. Amazon's Elastic Compute Clout (Amazon EC2), is a virtual computing environment that provides resizable compute capacity via the Internet.

In July 2009 this effort resulted in the launched of Key Bridge's first FCC Rules-compliant prototype channel list query responder. Continued testing and feedback during the summer allowed Key Bridge to launch in October 2009 its first operational, FCC Rules compliant TV band channel-list Web service that supports the open Internet standards described in this document.

Since October 2009, Key Bridge has collaborated with a limited number of end users to test the Database, its component subsystems and assorted web service. The Key Bridge team has

continued add convenience features, increase Web service and Web portal performance, and implement security.

Most components of the Key Bridge TV bands database solution are now operational on the Amazon EC2 cloud compute platform and ready for testing by the TV bands community.

The Phase 0 solution architecture in a cloud-compute environment, shown in Figure 51, contains all the system components of the solution architecture for carrier-grade communication services. It is functionally identical to a physical installation except for the hardware-accelerated performance features.

The Phase 0 system is very flexible and ideally suited for interoperability testing, device certification and feature enhancements during the early stages of TV band technology development.

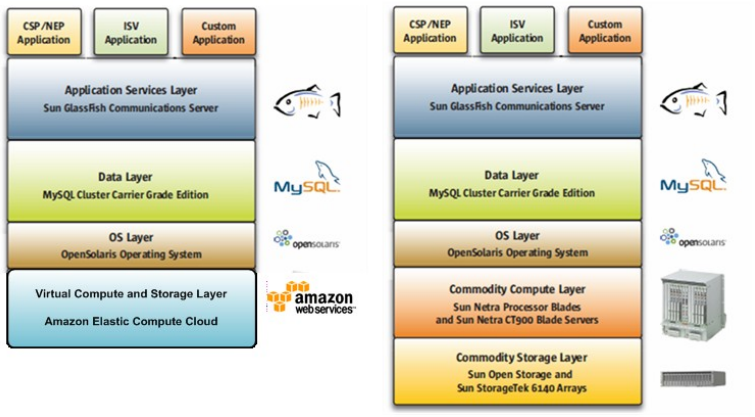


Figure 51: The Phase 0 implementation in a cloud-compute environment on the left is functionally complete but lacks the hardware-accelerated performance of a dedicated physical installation, shown on the right.

7.2 Phase 1: Commercial Introduction and Early Adoption

The Key Bridge Team actively engages with TV bands hardware manufacturers for interoperability coordination and testing. Phase 1 implementation will coincide with the first TV band devices receiving FCC certification. Its timing will assure that full-scale TV band services are online when the first certified devices become commercially available.

In Phase 1, the Key Bridge team will install its first physical system node at the Equinix collocation facility in Ashburn, VA. The first physical installation will incorporate all of the technology development from Phase 0 and bring significant performance improvements from hardware acceleration of security, encryption and database clustering.

With Equinix, the Key Bridge Team has company with unmatched infrastructure management capabilities. Equinix is widely recognized as the World's leading provider of network-neutral data centers and Internet exchange services. Equinix International Business Exchange™ (IBX®) centers lead the industry in quality and performance, with a proven record of industry-leading uptime.

Phase 1 implementation also maintains the Amazon EC2 cloud-based development node created in Phase 0 for continued software and services development, test and certification.

Phase 1 also calls for a new Amazon EC2 cloud-based production node. The cloud-based node is paired with the new physical installation at Equinix, Ashburn with interconnected security domains and enclaves. The could-based node mirrors all of the applications and functionality of

a physical node but without the same high-performance due to the absence of hardware-acceleration.

The two systems synchronize in near real-time and create an aggregate production system with load balancing capability and geographic and logical diversity for high availability TV band service. Figure 52 shows the detailed operations of the two-node system, where a high-availability Fortinet firewall cluster receives and routes all requests from various TV band clients. Depending upon system load, client requests can be directed to one or the other Node. In the example shown, a database synchronization request is directed to the cloud-based node instance.

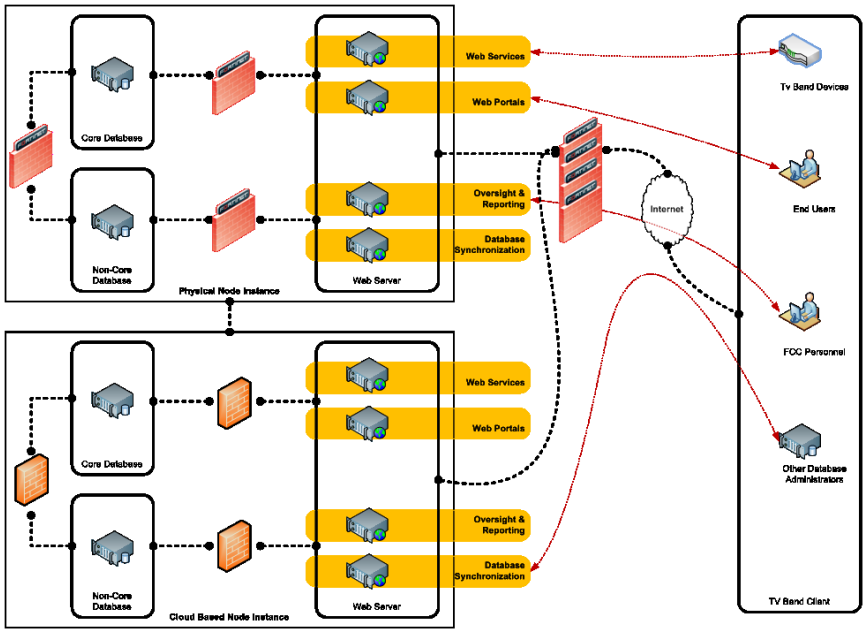


Figure 52: Phase 1 implementation is a single physical installation with load sharing, failover and backup provided by a software-based Node within the Amazon cloud.

7.3 Phase 2: Supporting Rapid TV Bands Adoption

The TV bands system is compute process intensive. Calculating protected service contours at high volume and high speed requires significant computer processor capacity. The Key Bridge

team implementation plan calls for Phase 2 to begin when the Phase 1 systems reach an average 50% of sustained compute resource utilization.

Choosing 50% utilization allows Key Bridge to match resource deployment with market demand, while providing enough time to ensure that sufficient infrastructure capacity is always available.

In Phase 2, the Key Bridge Team installs and commissions the remaining two physical nodes at Equinix facilities in San Jose, CA and Chicago, IL.

The new installations will incorporate all of the technology development from Phase 1 will bring significant performance improvements from load balancing across geographic and logically diverse application resources.

The final two facilities complete the Key Bridge reference architecture, and provide a fully redundant infrastructure with high availability, multiple levels of system redundancy, geographic diversity, distributed load sharing, and no single point of failure.

The four Nodes synchronize in near real-time and create an aggregate production system with load balancing capability and geographic and logical diversity for high availability TV band service. Figure 53 shows the final configuration of the four-node system, where each node is interconnected via a dedicated virtual private network. Network nodes share administrative data to coordinate handling client requests and assure service availability with load balancing, backup, failover and recovery.

Phase 2 maintains the Amazon EC2 cloud-based development node created in Phase 0 for continued software and services development, test and certification.

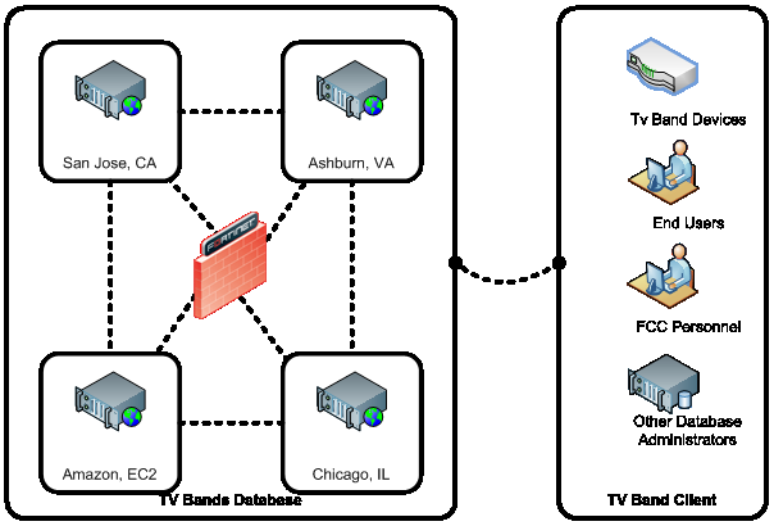


Figure 53: Phase 2 implementation completes the Key Bridge Team's solution architecture with four system nodes providing load balancing, geographic diversity, redundancy and failover for always-on TV band service.

7.4 Strategy for Long Term Growth

The Key Bridge Team believes a system of three physical and one virtual nodes provides sufficient geographic and logical diversity for a robust, always-on TV bands infrastructure. Our modular software and hardware architecture plus fine grained security strategy allow for easy capacity expansion to accommodate new features, new protections, responsive security, increased traffic and changing compute demands as the TV bands market evolves.

The Key Bridge operations plan calls upgrading system nodes when their average compute resource utilization reaches 50%. This allows us to match capital expenditures with market growth while assuring sufficient infrastructure is readily available to meet user demand.

A key benefit of the Key Bridge modular software architecture, adoption of the Java EE framework, hardware selection and fine-grained security strategy is the ease of upgrading system Nodes. Node capacity can be rapidly increased without affecting service availability. Additional computer systems can be added during a maintenance window, when system utilization is at a minimum, and applications seamlessly migrated to the new computers.

- Database capacity is increased by adding new commodity systems into the computer cluster
- Disk storage capacity is increased by adding additional commodity storage systems to the storage pool
- Application compute capacity is increased by node splitting, where new computers support a complete or partial set of system applications, depending upon resource demand and administrator planning.

The Web Container framework handles all database connection pooling plus application clustering and load balancing. Custom individual applications are easily migrated to new physical computers.

Figure 54 shows an example where three out of five servlet applications are migrated to a new computer system labeled “Web Services 2”. Servlet applications are modular and relatively autonomous, whereas the application server requires installation-specific configurations. Servlet capabilities are automatically exposed as web services on the new server and ready to service incoming requests. The process is completely transparent to the end user.

The Key Bridge implementation and operations plan calls for successive Node splits at the three physical installation sites to meet market demand. If future conditions require, Key Bridge can also extend the four-node architecture with additional physical sites where necessary.

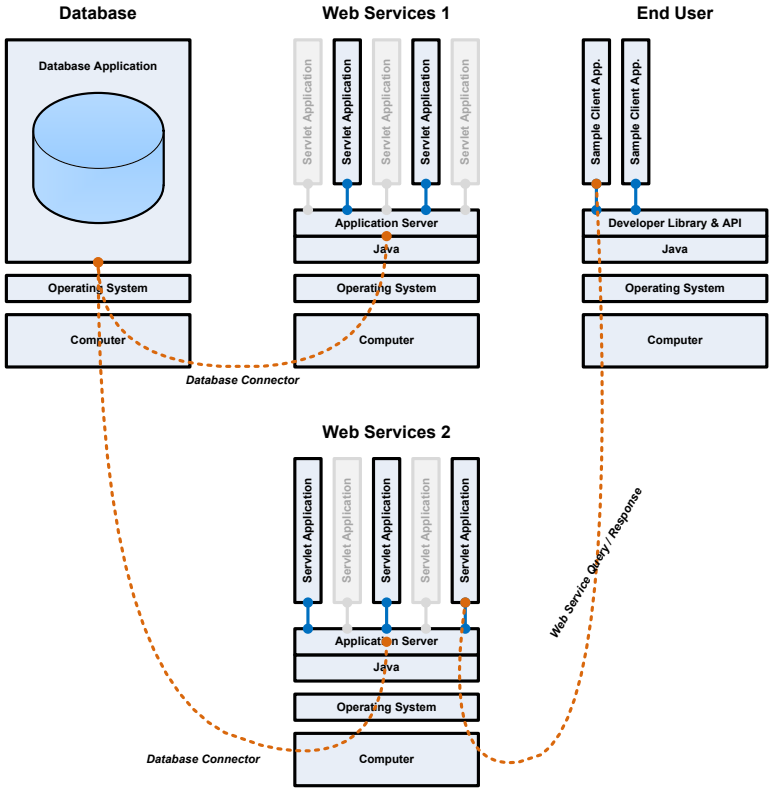


Figure 54: Node splitting is when a new physical computer is added and server applications are migrated to the new computer. Web Services 1 and 2 can support a full complement of server applications and share the load or may run a subset to isolate certain functions.

7.5 System Operations

Key Bridge TV band database operations will be collocated with AWS Convergence Technologies, Inc. (AWS). AWS's contribution to the Key Bridge Team is a robust and fully staffed operations center with established operating procedures, methods and practices that yield average service availabilities above 99.9%. In fact, the AWS Total Lightning Network, operated

under its WeatherBug brand, currently boasts an operational an operational availability record of 100 percent. The AWS / Key Bridge Operations Team consists of 20 highly skilled professionals who currently provide 24/7 support for mission critical information services to thousands of business clients and partners.

Key Bridge and AWS have a comprehensive operational strategy that provides high performance and high availability application services with integrated systems management, monitoring and service assurance resources.

Sun's System design elements like redundant and hot-swappable components, end-to-end data protection, advanced CPU and memory error detection and recovery, Dynamic Domains, and fault isolation through system clustering create an easily maintained infrastructure.

System administrators and network operators are principally responsible for assuring service availability. Highly skilled and trained staff provide rapid problem and fault resolution. Key Bridge and AWS have a proven record of accomplishment providing always-on Internet services.

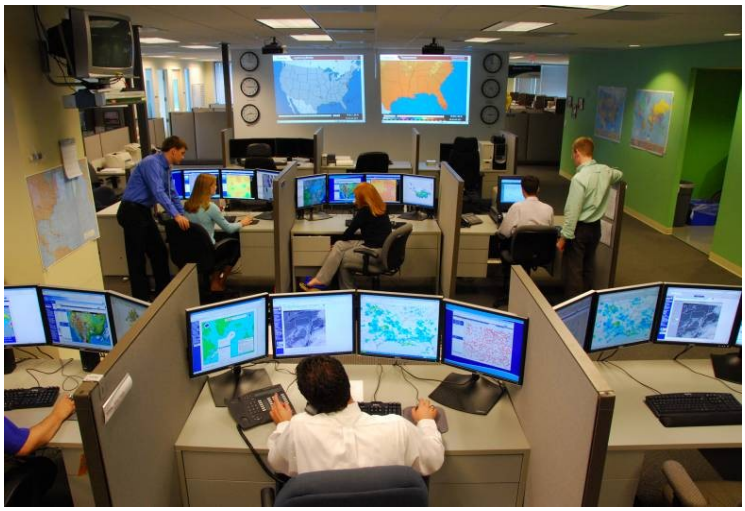


Figure 55: Key Bridge TV band system operations are collocated with the AWS network management team, who already manage computers in multiple centers and handle over three billion information requests every day.

7.5.1 Customer Service and Technical Support

TV band customer service and technical support staff are collocated with the AWS Meteorological Services group, an organizations that currently provides round-the-clock support for operations and customer service.

Throughout Phase 0 and Phase 1 of our implementation, Key Bridge and AWS will develop administrative procedures and technical guidelines to support the TV band user community's evolving requirements. We provide telephone and email support for customers and business partners covering interoperability, software troubleshooting and support, account management, information reporting and general operation according to the following schedule:

Schedule	Support Function
24 x 7 x 365	Operations support of all TV Bands system infrastructure,

	connectivity and service availability
8 a.m. to 6 p.m. EST M-F	Telephone and email support for all Web portal and Web service troubleshooting
24 x 7 x 365	Emergency telephone and email troubleshooting support for select Web portals and Web services like account management and channel lists

8 Commercialization Strategy

The Key Bridge Team supports the FCC's original intent and present TV bands strategy to foster competition among more than one fully qualified database administrator. [23] While we may provide unbundled services if the Commission authorizes partially competent information service providers, we do not believe they create meaningful value in the first few years of TV bands market adoption.

8.1 Acquisition Plan for Phase 0, 1 and 2 Infrastructure

In 2009, the Key Bridge Team began implementation of Phase 0 and committed most of the capital investment necessary to design, implement, deploy and test a functional TV bands database system.

Phase 0 system architecture, software design, hardware specification, management procedures, developer resources, and testing plans are complete and ready for commercial deployment.

8.2 Payment Options for Registration Fees

In earlier communications with the FCC, Key Bridge described concerns that the TV band rules should foster a TV bands marketplace where consumer incentives align with FCC goals like interference avoidance, price competition and commercial sustainability.[24]

Since 2009 Key Bridge has engaged with the TV band hardware manufacturing and wireless service provider communities to establish streamlined processes for device registration. We have

---

[23] See Key Bridge, ET Docket 04-186, *Opposition to Petitions for Reconsideration*

[24] See Key Bridge ex-parte dated October 02, 2009.

also worked to identify and reduce unnecessary cost factors that contribute to higher fee levels. Key Bridge will provide two options for the payment of Fixed TV band device registration fees: pre-paid and ad-hoc.

8.2.1 Options for Pre-paid TVBD Registration

Only Fixed TVBD require unlicensed registration. Fixed TVBD registration is principally a business-to-business relationship with standard commercial contract terms and invoicing.

FCC Rules anticipate that Fixed TVBDs create wireless network infrastructure for other "client" devices to access, and that Fixed devices will likely require a professional installer. A responsible party, i.e. the professional installer, must register the Fixed TVBD with a TV bands database prior to use. Registration includes information about the technical details of the device, a responsible party, and payment of a fee.

The Key Bridge pre-paid program presents a lower total cost of ownership (TCO) solution over ad-hoc registration and includes two attractive features that hardware manufacturers and network service provider's desire: transferability and repeatability.

Transferability

Pre-paid registrations with Key Bridge are assigned to the TV band device and may be transferred if the device is sold to a new owner. Transferability maintains the residual value of used hardware and benefits both manufacturers and wireless service providers. Transferability makes a manufacturer's product more attractive and may allow a small price premium or competitive advantage. Following a network upgrade, operators typically sell their old equipment on the secondary market. Transferability allows wireless service providers to sell fully functional equipment and recapture additional value from such sales.

Repeatability

Repeatability entitles a Fixed TV band device to re-register with the Key Bridge Database by the same owner any number of times. Repeatability provides wireless operators with the flexibility they need to reposition their network infrastructure and respond to evolving service demands without incurring any additional deployment expense.

Wireless network operators communicated to Key Bridge their concern that device registration fees could complicate network upgrades, where equipment is often repositioned to accommodate demand and technology introduction. Because of these conversations, pre-paid device registrations with Key Bridge are infinitely repeatable.

8.2.2 Support for Ad-Hoc Fixed TVBD Registration

Ad-hoc registration serves as a catchall, supporting any type of end user and any type of device, including large and small wireless operators, individual users and new or used TV band devices. Ad-hoc TVBD registrations are simple to establish but not transferrable or repeatable. Rather, an ad-hoc registration record binds a specific device, responsible party and operating location together and authorizes it to receive valid channel lists.

Ad-hoc registration is available through a Web portal. Maintaining a commercial account is not necessary as the users pays the registration fee at the conclusion of device registration by online checkout.

8.3 Payment Options for Channel List Fees

Current rules entitle the Database to charge fees for channel list transactions to cover its cost of operation.[25] As a practical matter, implementation may potentially require millions of Mode-II consumers to maintain a commercial account with a Database administrator to pay for channel list fees. The Key Bridge solution supports several channel-list fee payment options for maximum flexibility and accommodation to the Fixed and Mode-II user communities.

Key Bridge provides three flexible payment structures and we are prepared to modify these and create additional structures as the White Spaces ecosystem matures. Presently supported options include:

- Pre-paid, Flat-rate Contracts
- Agency Accounts
- Ad-Hoc Accounts

[25] 47 CFR §15.714

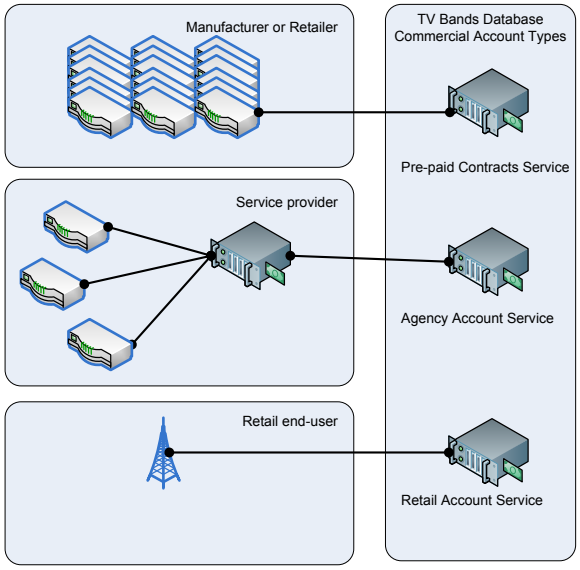


Figure 56: Key Bridge will support three payment options for channel-list fees. This provides needed flexibility and accommodation to the Fixed and Mode-II user community.

8.3.1 Support for Pre-paid, Flat-Rate Channel List Services

In this scenario, payment of a one-time fee establishes a transferrable contract entitling the TV band device to channel list services for its usable life. Pre-paid channel-list services have several benefits for hardware manufacturers, wireless operators and consumers. Principal among them is convenience. Consumers and end users of Mode-II devices may simply plug-and-play, with no activation procedure or fees. Another benefit is cost. Key Bridge will offer a significant discount on pre-paid service contracts when compared with the long-term cost of ad-hoc operation.

Fee payment may occur at the time of manufacturer, point of sale or registration. For integrated operations like high-volume manufactures or retail outlets, payment is by business-to-business merchant services. For single device activation by consumers or professional installers, payment is by online checkout, which supports corporate accounts or credit and debit cards.

The TV bands community generally regards a pre-paid service contract as the most desirable payment option.

8.3.2 Support for Agency Accounts

Key Bridge may support agency account services for wireless service providers to aggregate the collection and payment of channel list fees for their uses. This option offloads account management and payment requirements from the consumer to the service provider.

8.3.3 Support for Ad-Hoc Accounts

For Mode-II devices that are not associated with a participating service provider, Key Bridge may support ad-hoc retail account management for Fixed and Mode-II devices that cannot be accommodated by other options.

Charging consumers for individual channel query transactions may create a nuisance for consumers, an unnecessary and expensive provisioning and billing burden on the administrator, and a strong incentive for consumers to undermine system security. Key Bridge therefore does not intend to offer single ad-hoc channel query services or support micro-payments for single-transactions or short time periods. Ad-hoc TV band services are only available for one, two and three-year terms. All service contracts are available to users of any certified TV band device on a non-discriminatory basis for a fixed, flat fee. When a customer is ready to make a purchase, they can pay with their credit card or through their PayPal or Google checkout account. Payment providers handle payment transactions directly, and customers receive electronic confirmation.

Fraud protection policies protect consumers against unauthorized purchases. Consumer's purchase history and full credit card number are kept confidential and not shared with the database administrator.

9 The Key Bridge TV Bands Solution

Key Bridge has assembled a solution with industry leading companies that bring the technology, infrastructure, resources, expertise and personnel needed to develop, deploy and maintain state-of-the-art TV band services.

After reviewing the competitive landscape, Key Bridge chose Sun and Oracle as our preferred supplier of commercial hardware and software technology. Sun and Oracle today are the largest contributors of open source technology and provide always-on infrastructure solutions to 100% of the Fortune 100.

Key Bridge worked with industry's largest and most reliable service providers to develop a comprehensive plan for implementation, collocation and connectivity. Amazon's cloud compute resources enable rapid startup and technology development, while Equinix and AWS provide a stable foundation necessary to deploy, connect and manage mission-critical, always-on infrastructure.

Fortinet, the worldwide leader of network security appliances, provides a fine-grained security architecture and integrated strategy for secure, reliable operation. Fortinet technologies protect

the TV bands ecosystem, provide standards-compliant and scalable security, while preserving needed flexibility for rapid innovation and development.

Symantec brings to the team a world-class expertise and capabilities for signed digital certificates, public key infrastructure, secure identity management and fraud detection. Symantec, through its acquisition of VeriSign Security, provides Secure Sockets Layer (SSL) Certificate Services, the Public Key Infrastructure (PKI) Services, the VeriSign Trust Services and the VeriSign Identity Protection (VIP) Authentication Service.

Key Bridge will contract with FirstData to provide flexible and convenient payment options for consumers and businesses. Key Bridge also intends to provide Google Checkout and PayPal options for supporting online consumer payment.

9.1 Key Bridge Global LLC

Established in 2001, Key Bridge Global LLC is a privately held Virginia company providing systems integration, custom software, research and development and professional services to companies, the U.S. Government, and the U.S. Military. Our core business is the development and strategic application of new technologies to solve customer problems.

Key Bridge also develops many original and unique products, services and intellectual property through internally funded research and development. Applications range from innovative approaches to inter-satellite communications and formation flying to unmanned aerial vehicle detection, voice over IP security architectures and improved wireless waveforms. We are also a leading developer of spectrum administration technologies which will provide unique and useful functionality for cognitive radios and dynamic spectrum access systems.

Key Bridge is headquartered in McLean, VA.

9.2 Oracle

For almost 30 years, Oracle has been helping customers manage their business systems and information with reliable, secure, and integrated technologies.

Today, Oracle is the largest business software company in the world, with 345,000 customers—including 100 of the Fortune Global 100—and supports these customers in more than 145 countries.

Oracle Inc., Inc. (NASDAQ: ORCL) provides network computing infrastructure solutions that include computer systems, software, storage and services. Its core brands include the Java technology platform, the Solaris operating system, MySQL, StorageTek and the UltraSPARC processor.

By investing in research and development, Oracle creates products and services that address the complex issues that customers face today, including increasing demands for network access, bandwidth and storage being driven by explosive growth in network participation and sharing. Sun innovates at all levels of the system and partners with market leaders to provide value and choice for its customers.

Oracle's network computing infrastructure solutions are used in a wide range of industries including technical/scientific, business, engineering, telecommunications, financial services, manufacturing, retail, government, life sciences, media and entertainment, transportation, energy/utilities and healthcare.

9.3 MySQL AB

MySQL is the world's most popular open source database software, with over 100 million copies of its software downloaded or distributed throughout its history. With its superior speed, reliability, and ease of use, MySQL has become the preferred choice for Web, Web 2.0, SAAS, ISV, Telecom companies and forward-thinking corporate IT Managers because it eliminates the major problems associated with downtime, maintenance and administration for modern, online applications.

Many of the world's largest and fastest-growing organizations use MySQL to save time and money powering their high-volume Web sites, critical business systems, and packaged software — including industry leaders such as Yahoo!, Alcatel-Lucent, Google, Nokia, YouTube, Wikipedia, and Booking.com.

The flagship MySQL offering is MySQL Enterprise, a comprehensive set of production-tested software, proactive monitoring tools, and premium support services available in an affordable annual subscription.

The MySQL database is owned, developed and supported by Oracle Inc., one of the world's largest contributors to open source software.

9.4 Fortinet

Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure.

Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

Fortinet's flagship FortiGate® security platforms offer a powerful blend of ASIC-accelerated performance, integrated multi-threat response, and constantly-updated, in-depth threat intelligence. Employing innovative technologies for networking, security and content analysis, Fortinet systems integrate the industry's broadest suite of security technologies, including firewall, VPN, antivirus, intrusion prevention (IPS), Web filtering, antispam, and traffic shaping,

all of which can be deployed individually to complement legacy solutions or combined for a comprehensive threat management solution. The company complements these solutions with an array of management, analysis, e-mail, database and end-point security products.

Fortinet has shipped more than 450,000 appliances to more than 75,000 customers worldwide, including:

- 55 of the Global 100
- 7 of the top 10 Fortune companies in Americas
- 9 of the top 10 Fortune telecommunications companies
- 9 of the top 10 Fortune banking companies
- 7 of the top 10 Fortune defense/aerospace companies

9.5 Symantec

Symantec (NASDAQ: SYMC) was founded in 1982 by visionary computer scientists. The company has evolved to become one of the world's largest software companies with more than 17,500 employees in more than 40 countries. We provide security, storage and systems management solutions to help our customers – from consumers and small businesses to the largest global organizations – secure and manage their information-driven world against more risks at more points, more completely and efficiently than any other company. Symantec helps consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec offers authentication solutions for government including PKI, two-factor authentication, and digital certificates that have been certified to meet the highest technical and policy standards of the United States Government. They are approved for deployment to Federal, state, and local agencies and government contractors.

As business processes become more integrated and self-service becomes the norm, enterprises are opening closed networks to business partners, customers and the mobile workforce. To reduce risk and comply with security regulations, companies rely on public key infrastructure (PKI) and digital certificates. PKI is a collection of components and policies needed to issue, manage, and revoke digital certificates, used to authenticate any application, person, process, or organization in an enterprise network, extranet, or on the Internet. Symantec leads the industry with trusted PKI solutions that reduce the complexity of securing today's mission-critical interactions. With PKI solutions, Symantec provides the unmatched flexibility and scalability that global enterprises as well as regional, federal, and international governments need to meet a broad range of business and operational requirements.

9.6 AWS Convergence Technologies, Inc.

Founded in 1992, WeatherBug, a brand of AWS Convergence Technologies, Inc. ensures individuals, schools, businesses and government agencies receive the most precise live weather conditions, the most relevant weather reports, and the earliest weather warnings to safeguard property, lives and to plan ahead with confidence.

With 8,000 Weather Tracking Stations and more than 1,000 cameras primarily based at neighborhood schools and public safety facilities across the U.S., WeatherBug maintains the largest weather network in the world.

WeatherBug delivers live weather data to millions of consumers via the Internet, and to more than 100 state and local government agencies including the National Weather Service, and to broadcast television stations, schools, and businesses. WeatherBug data reaches over 80 million households every month.

AWS is headquartered in Germantown, MD.

WeatherBug's Professional products leverage the full power of the WeatherBug Network to deliver real-time weather solutions. Thousands of professional, governmental and educational organizations, including the National Weather Service, rely on WeatherBug to make more informed mission critical decisions that safeguard lives, impact communities and improve business operations. With a comprehensive suite of offerings, WeatherBug Professional delivers:

- Time and mission critical weather information services to NOAA (US government) agencies including the National Weather Service, Air Resources Laboratory, Global Systems Division and National Severe Storms Laboratory for real-time storm tracking and dispersion modeling
- Alerting, severe weather forecasting, graphical visualization and GIS services to state and local public safety agencies nationwide including fire, police and emergency management
- Decision support products and services to commercial enterprise customers including utilities and energy traders for protection of multi-billion dollar distributed assets and financial transactions

- Supplemental math and science curriculum to over 3,000 public and private schools

9.7 Amazon Web Services

Since early 2006, Amazon Web Services (AWS) has provided companies of all sizes with an infrastructure web services platform in the cloud. With AWS, companies can requisition compute power, storage, and other services in a suite of elastic IT infrastructure services as demands require.

AWS provides a user-defined development platform and programming model with no up-front expenses or long-term commitments. AWS is the most cost-effective way to develop and deliver new web application to customers and clients.

AWS is built on Amazon.com's global computing infrastructure, that is the backbone of Amazon.com's $15 billion retail business and transactional enterprise whose scalable, reliable, and secure distributed computing infrastructure has been honed for over 13 years.

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. It makes web-scale computing easier for developers.

Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing quick scale capacity as computing requirements change. Amazon EC2 provides developers tools to build failure resilient applications and isolate themselves from common failure scenarios.

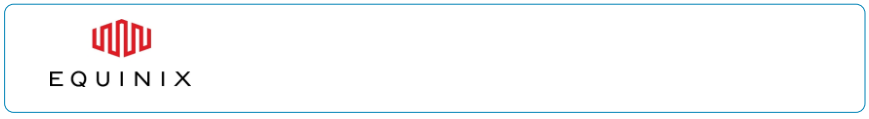
Developers may chose from multiple instance types, operating systems, and software packages. Amazon EC2 accommodates different system configurations with memory, CPU, instance storage, and the boot partition size that are optimal for each operating system and application.

Amazon EC2 offers a highly reliable environment where replacement instances can be rapidly and predictably commissioned. The service runs within Amazon's proven network infrastructure and datacenters. The Amazon EC2 Service Level Agreement commitment is 99.95% availability for each Amazon EC2 Region.

Secure – Amazon EC2 provides numerous mechanisms for securing compute resources.

- Firewall settings that control network access to and between groups of instances.
- Compute isolation and industry-standard encrypted IPsec VPN support
- Geographic diversity across in multiple locations

9.8 Equinix



Equinix, Inc. (Nasdaq: EQIX) operates International Business Exchange™ (IBX®) data centers across 18 markets in North America, Europe, and Asia-Pacific. Global enterprises, content and financial companies, and network services providers rely upon Equinix's insight and expertise to protect and connect their most valued information assets. The ideas on which we were founded remain just as true today in our mission to ensure the vitality of an ever growing, information-driven world.

Equinix is the preferred destination for the mission-critical operations of the world's most demanding businesses.

- We consider it our responsibility to safeguard our customers' business within our International Business Exchange (IBX®) data centers—the most reliable in the industry.
- Our customers rely on the unique ecosystem of major networks and business partners within our IBX centers to connect to their stakeholders and end-users.
- Our team of professionals has configured data center installations for some of the most sophisticated businesses in the world.

9.9 Level-3

Level 3 Communications® is an international communications company headquartered in Broomfield, Colorado. The company operates one of the world's largest communications and Internet backbones over an advanced, IP-optimized network.

Level 3 is focused on delivering premier data, video and voice services — for open IP Tone capabilities to businesses and carriers. We offer a comprehensive portfolio of network offerings that spans Internet Protocol (IP) services, broadband transport, collocation services, and patented Soft switch-based managed modem and voice services. Level 3 also uses these network services as a foundation for delivering enterprise telecommunications solutions.

Level 3 supports its customers across four groups:

- Level 3 Wholesale Markets serves national and global service providers with integrated data, voice, and video services across one of the world's largest, most-modern networks.

- Level 3 Content Markets combines broadcast and advertising distribution services with traditional Internet services to help rich-media content providers operate at a huge scale among multiple destinations.
- Level 3 Business Markets connects regional enterprises, local service providers, and regional carriers with high-availability, nationwide network access and high-performance data, voice and Internet solutions.

Level 3 counts among its customers:

- 19 of the world's top 20 telecom companies
- 9 of the top 10 U.S. Internet Service Providers (ISPs)
- 9 of the top 10 U.S. cable companies
- Top 5 U.S. Wireless Service Providers

9.10 FirstData

First Data is a global technology and payments processing leader, serving more than 5 million merchant locations, 2,000 card issuers and their customers and millions of consumers worldwide. Whether the choice of payment is a gift card, a credit or debit card or a check, First Data securely processes the transaction and harnesses the power of the data to deliver intelligence and insight for its customers.

Financial institutions, large and small businesses as well as government agencies rely on First Data to empower them to build stronger, more profitable customer relationships as commerce continues to transform.

Our innovations in secure infrastructure, intelligence and insight empower our customers to move beyond “electronic payments” to embrace data-driven commerce, which incorporates data intelligently into every transaction.

First Data’s strategic focus is on delivering innovations in prepaid, eCommerce and mobile payments solutions. First Data also provides payment-processing solutions such as fraud protection and authentication solutions, check guarantee and verification services and point-of-sale (POS) devices and service.

9.11 Consumer Payment Providers

Google checkout and Paypal contribute standard merchant services to the Key Bridge solution, where web site users can quickly and easily pay for Web-based with a range of payment options including: credit card, debit card, electronic funds transfer, bank check and online accounts.

When a customer is ready to make a purchase, they can pay with their credit card or through their PayPal or Google checkout account.

Payment providers handle payment transactions directly, and customers receive electronic confirmation.

Both company’s fraud protection policies protect consumers against unauthorized purchases. Consumer’s purchase history and full credit card number are kept confidential and not shared with the database administrator.

10 Commitment to Neutrality

One of the greatest things about the Internet is that nobody really owns it: it is a global collection of networks, both big and small. Connected together, private networks form the Internet, a public and open resource for communication and data exchange.

However, just because nobody owns the Internet, does not mean it is ungoverned, monitored or maintained. Several organizations like the Internet Society, the Internet Corporation for Assigned Names and Numbers (ICANN), and the World Wide Web Consortium (W3C) oversee the formation of policies and protocols that define how we use and interact with the Internet.

As with the Internet, the White Space community includes individuals and organizations who wish to see a viable, stable, secure Television Band ecosystem that fosters innovative wireless products and services.

Similar to other Internet resources like domain names and IP addresses, unlicensed TV band channels represent a limited resource upon which Internet infrastructure will be built. Key Bridge agrees with the FCC that that TV band services are delivered on a non-discriminatory basis and that TV band resources must be governed by a set of neutral commercial policies to everyone's benefit.[26]

The Key Bridge Team is not aligned to any particular interest group and our solution is a neutral television band database administrator. Key Bridge commercial policy is to:

- implement the letter and spirit of Commission rules, and
- provide robust incumbent protection from interference, and

[26] See requirements for non-discrimination at 47 CFR §15.714(g)

- publish available spectrum for unlicensed operation on a nondiscriminatory basis.

10.1 Innovation and Open Source

Open source plays an important role in software innovation, where new methods, techniques and improvements iteratively build on their predecessors. Open source software also benefits from community supported bug tracking and algorithm development, where software source code benefits from multiple sources of quality assurance and testing.

Much of the Key Bridge solution and many members of the Key Bridge team are significant contributors of open source technologies. After receiving authorization, Key Bridge intends to publish components of our custom software as open source and invite the Internet community to review, develop and improve the television administration system.

Key Bridge software will be available with revision control, which enables distributed source code development and simplifies incorporation of community provided improvements and bug fixes. A bug-tracking system will allow community developers and end-users to submit bug reports directly to Key Bridge developers for analysis and correction.

11 Closing Summary and Statement of Compliance

The Key Bridge Team is pleased to submit this revised proposal to administer a database of the unlicensed Television broadcast bands. The many technologies brought together in our solution are proven and tested to integrate together. The infrastructure components, system architecture and network design called for in the Key Bridge Team's database solution currently support millions of network users and billions of dollars in online commerce safely, securely and reliably.

Our neutral approach and our open systems architecture incorporate many suggestions, recommendations, and requirements gathered through extensive collaboration with a wide spectrum of interested parties over several years. The Key Bridge Team's solution completely satisfies all of the FCC's current requirements. It is also flexible enough to accommodate future changes or modifications to those requirements.

The Key Bridge Team is happy to provide any additional information the Commission may require to evaluate our proposed solution.

/s/

Jesse Caulfield

Key Bridge Team Leader

Amazon Web Services	*Key Bridge Global LLC*	*Symantec Inc.*
Equinix Inc.	*Level (3) Communications*	
Fortinet Inc.	*Oracle Inc.*	

12 Appendix: Mutual Authentication

Mutual Authentication is a security procedure wherein a TVBD must prove its identity to a Database and the Database must prove its identity to the TVBD before a connection is established between the two. Mutual authentication requires that the TVBD and Database prove their respective identities to each other before connecting or accepting information from each other. Identity can be proved using cryptographic means like public key infrastructure or the exchange of public keys.

HTTP basic authentication is not particularly secure. Basic authentication can unencrypted expose user names and passwords. HTTP mutual authentication does not expose identifying information. Instead, the server and the client authenticate each other with pre-shared keys or certificates.

There are two basic types of mutual authentication:

- Certificate-based mutual authentication
- User name- and password-based mutual authentication

The Key Bridge security solution employs certificate-based mutual authentication by default, and username/ password authentication only as a backup method.

As background, conventional HTTP Basic Authentication requires that a server request a user name and password from a web client and then verify that the user name and password are valid by comparing them against a database of authorized users. Basic HTTP authentication is illustrated in fig x and includes the following actions:

1. A client requests access to a protected resource.
2. The web server returns a dialog box that requests the user name and password.

3. The client submits the user name and password to the server.
4. The server authenticates the user in the specified realm and, if successful, returns the requested resource.

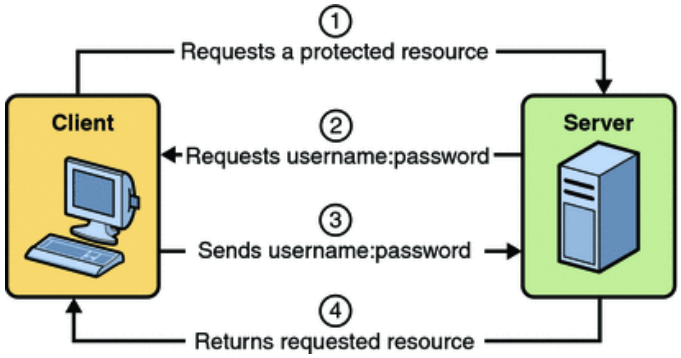


Figure 57: HTTP Basic Authentication

The certificate-based mutual authentication process involves two sets of public/private key pairs: one for the server and one for the client. In Figure 58 the private keys are stored in the client and servers respective key store and their public keys are published to an external PKI, or trust store. When pre-shared keys are used public keys are exchanged beforehand and stored in each other's respective key store.

The authentication transaction process is:

1. A client requests access to a protected resource
2. The web server presents its certificate to the client
3. The client verifies the server's certificate locally (with a pre-shared key) or remotely (via PKI)
4. If successful, the client sends its certificate to the server
5. The server verifies the client's credentials locally (with a pre-shared key) or remotely (via PKI)

6. If successful, the server grants access to the protected resource requested by the client

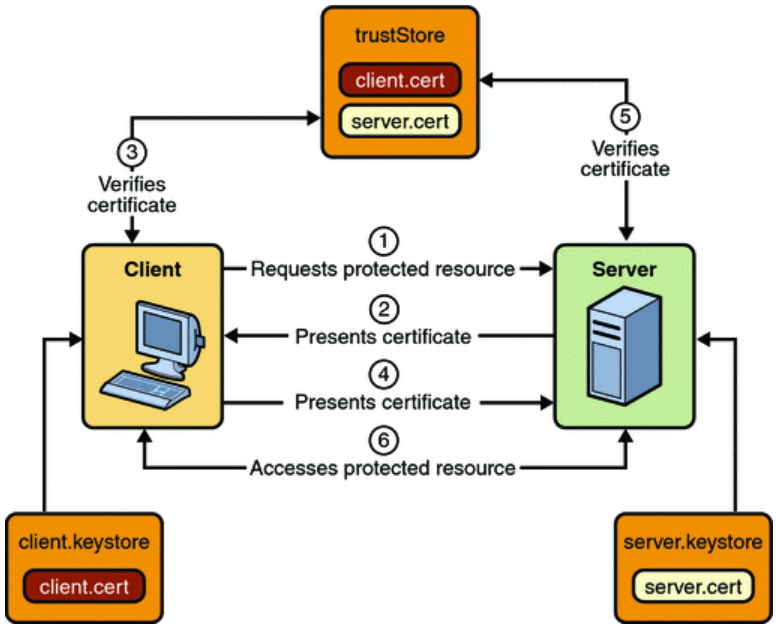


Figure 58: Certificate-based mutual authentication with public key infrastructure. For pre-shared keys the client.cert and server.cert are stored in the server.keystore and client.keystore, respectively.

It is also possible to implement user name and password based mutual authentication, where the FCC ID and serial number represent a username and password. Both would have to be registered prior to authentication.

In username and password mutual authentication only the server (Database) has a certification. The process is as follows:

1. A client requests access to a protected resource.
2. The web server presents its certificate to the client.
3. The client verifies the server's certificate.

4. If successful, the client sends its user name and password to the server, which verifies the client's credentials.
5. If the verification is successful, the server grants access to the protected resource requested by the client.

All database communications are required to employ TLS-protected session and ensure that all message content is protected for confidentiality.

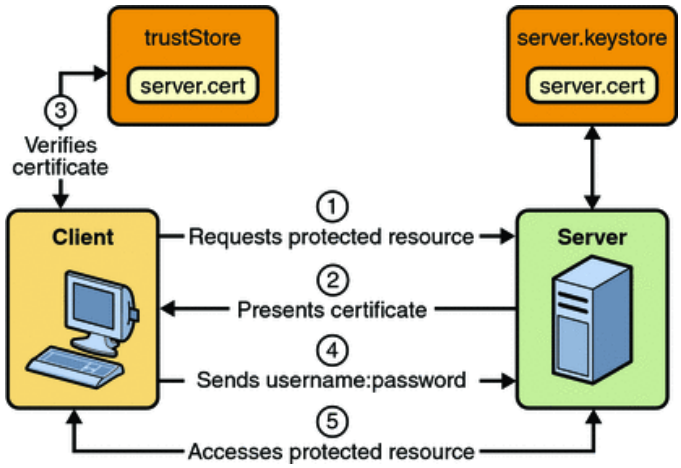


Figure 59: User name and password based mutual authentication